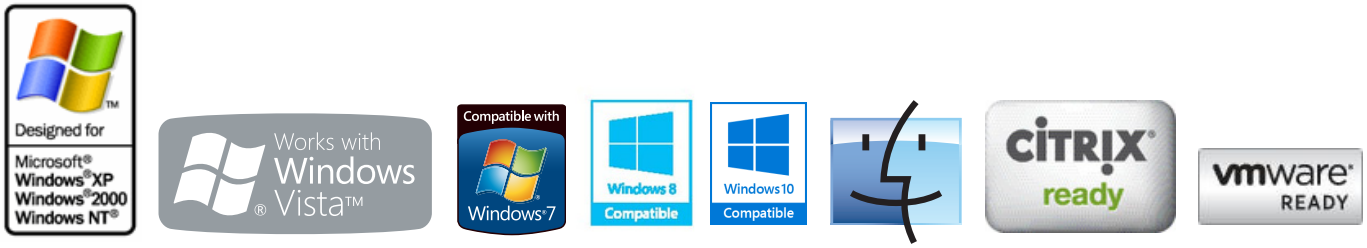
DeviceLock®

DLP Suite

User Manual

Software Version 8.1



© 1996-2015 DeviceLock, Inc. All rights reserved.

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means for any purpose other than the purchaser's personal use without the prior written permission of DeviceLock, Inc.

Trademarks

DeviceLock and the DeviceLock logo are registered trademarks of DeviceLock, Inc. All other product names, service marks, and trademarks mentioned herein are trademarks of their respective owners.

DeviceLock DLP Suite – User Manual
Software Version: 8.1
Updated: November 27, 2015

Contents

ABOUT THIS MANUAL 6
CONVENTIONS 6
OVERVIEW 7
GENERAL INFORMATION 7
MANAGED ACCESS CONTROL FOR DEVICES AND PROTOCOLS 11
DEVICELOCK SERVICE FOR MAC 17
UNDERSTANDING DEVICELOCK CONTENT SECURITY SERVER 18
HOW SEARCH SERVER WORKS 18
EXTENDING DEVICELOCK FUNCTIONALITY WITH CONTENTLOCK AND NETWORKLOCK 20
LICENSING 25
RECOMMENDED BASIC SECURITY MEASURES 26
INSTALLATION 27
REQUIREMENTS 27
DEPLOYING DEVICELOCK SERVICE FOR WINDOWS 29
INTERACTIVE INSTALLATION 29
UNATTENDED INSTALLATION 36
INSTALLATION VIA MICROSOFT SYSTEMS MANAGEMENT SERVER 38
REMOTE INSTALLATION VIA DEVICELOCK MANAGEMENT CONSOLE 38
REMOTE INSTALLATION VIA DEVICELOCK ENTERPRISE MANAGER 39
INSTALLATION VIA GROUP POLICY 41
INSTALLATION VIA DEVICELOCK ENTERPRISE SERVER 49
DEPLOYING DEVICELOCK SERVICE FOR MAC 51
INTERACTIVE INSTALLATION 51
COMMAND LINE UTILITY 54
UNATTENDED INSTALLATION 55
INSTALLING MANAGEMENT CONSOLES 56
INSTALLING DEVICELOCK ENTERPRISE SERVER 62
PLANNING INFRASTRUCTURE 63
INTERACTIVE INSTALLATION 63
INSTALLING AND ACCESSING DEVICELOCK WEBCONSOLE 80
INSTALLING DEVICELOCK CONTENT SECURITY SERVER 84
DEVICELOCK CERTIFICATES 100
OVERVIEW 100
GENERATING DEVICELOCK CERTIFICATES 100
INSTALLING/REMOVING DEVICELOCK CERTIFICATE 102
DEVICELOCK SIGNING TOOL 107
OVERVIEW 107

DEVICE CODE 107
SERVICE SETTINGS 109
DEVICELOCK MANAGEMENT CONSOLE 115
OVERVIEW 115
INTERFACE 117
CONNECTING TO COMPUTERS 118
POSSIBLE CONNECTION ERRORS 121
MANAGING DEVICELOCK SERVICE FOR WINDOWS 123
SERVICE OPTIONS 124
DEVICES 170
PERMISSIONS (REGULAR PROFILE) 170
AUDITING, SHADOWING & ALERTS (REGULAR PROFILE) 180
USB DEVICES WHITE LIST (REGULAR PROFILE) 190
MEDIA WHITE LIST (REGULAR PROFILE) 194
SECURITY SETTINGS (REGULAR PROFILE) 198
AUDIT LOG VIEWER (SERVICE) 201
SHADOW LOG VIEWER (SERVICE) 206
MANAGING DEVICELOCK SERVICE FOR MAC 213
ENABLING NTLM AUTHENTICATION FOR LOCAL USERS ON MAC OS X 215
MANAGING DEVICELOCK ENTERPRISE SERVER 218
SERVER OPTIONS 219
AUDIT LOG VIEWER (SERVER) 220
SHADOW LOG VIEWER (SERVER) 223
SERVER LOG VIEWER 227
MONITORING 229
MANAGING AND USING DEVICELOCK CONTENT SECURITY SERVER 243
NAVIGATING DEVICELOCK CONTENT SECURITY SERVER 243
CONFIGURING GENERAL SETTINGS FOR DEVICELOCK CONTENT SECURITY SERVER 245
CONFIGURING FULL-TEXT SEARCH SETTINGS FOR SEARCH SERVER 250
USING SEARCH SERVER 257
DEVICELOCK GROUP POLICY MANAGER 269
OVERVIEW 269
APPLYING GROUP POLICY 270
STANDARD GPO INHERITANCE RULES 270
STARTING DEVICELOCK GROUP POLICY MANAGER 271
USING DEVICELOCK GROUP POLICY MANAGER 275
USING RESULTANT SET OF POLICY (RSOP) 278
MANAGING DEVICELOCK SERVICE FOR MAC VIA GROUP POLICY 280
DEVICELOCK SERVICE SETTINGS EDITOR 281
OVERVIEW 281
DEVICELOCK ENTERPRISE MANAGER 283

OVERVIEW 283
INTERFACE 284
SCAN NETWORK DIALOG BOX 285
SELECTING COMPUTERS 285
SELECTING PLUG-INS 291
STARTING A SCAN 292
PLUG-INS 293
AUDIT LOG VIEWER 294
INSTALL SERVICE 294
REPORT PERMISSIONS/AUDITING 294
REPORT PNP DEVICES 296
SET SERVICE SETTINGS 297
SHADOW LOG VIEWER 298
UNINSTALL SERVICE 298
OPEN / SAVE / EXPORT 299
COMPARING DATA 300
FILTERING DATA 304
CONTENT-AWARE RULES FOR DEVICES (REGULAR PROFILE) 307
CONTENT-AWARE RULES FOR ACCESS CONTROL OPERATIONS 308
CONTENT-AWARE RULES FOR SHADOW COPY OPERATIONS 314
CONTENT-AWARE RULES FOR DETECTION OPERATIONS 317
CONFIGURING CONTENT DETECTION SETTINGS 318
FILE TYPE DETECTION CONTENT GROUPS 319
KEYWORDS CONTENT GROUPS 322
PATTERN CONTENT GROUPS 327
DOCUMENT PROPERTIES CONTENT GROUPS 332
COMPLEX CONTENT GROUPS 336
ORACLE IRM CONTENT GROUPS 339
VIEWING BUILT-IN CONTENT GROUPS 343
DUPLICATING BUILT-IN CONTENT GROUPS 343
EDITING AND DELETING CUSTOM CONTENT GROUPS 344
TESTING CONTENT GROUPS 345
MANAGING CONTENT-AWARE RULES 346
DEFINING CONTENT-AWARE RULES 346
EDITING CONTENT-AWARE RULES 350
COPYING CONTENT-AWARE RULES 351
EXPORTING AND IMPORTING CONTENT-AWARE RULES 352
UNDEFINING CONTENT-AWARE RULES 354
DELETING CONTENT-AWARE RULES 355
CONTENT-AWARE RULES FOR PROTOCOLS (REGULAR PROFILE) 356
CONTENT-AWARE RULES FOR ACCESS CONTROL OPERATIONS 356
CONTENT-AWARE RULES FOR SHADOW COPY OPERATIONS 359
CONTENT-AWARE RULES FOR DETECTION OPERATIONS 362
CONFIGURING CONTENT DETECTION SETTINGS 363

FILE TYPE DETECTION CONTENT GROUPS 364
KEYWORDS CONTENT GROUPS 367
PATTERN CONTENT GROUPS 372
DOCUMENT PROPERTIES CONTENT GROUPS 376
COMPLEX CONTENT GROUPS 380
ORACLE IRM CONTENT GROUPS 383
VIEWING BUILT-IN CONTENT GROUPS 386
DUPLICATING BUILT-IN CONTENT GROUPS 387
EDITING AND DELETING CUSTOM CONTENT GROUPS 388
TESTING CONTENT GROUPS 389

MANAGING CONTENT-AWARE RULES 390
DEFINING CONTENT-AWARE RULES 390
EDITING CONTENT-AWARE RULES 394
COPYING CONTENT-AWARE RULES 395
EXPORTING AND IMPORTING CONTENT-AWARE RULES 396
UNDEFINING CONTENT-AWARE RULES 398
DELETING CONTENT-AWARE RULES 399

PROTOCOLS (REGULAR PROFILE) 401

MANAGING PERMISSIONS FOR PROTOCOLS 402
SETTING AND EDITING PERMISSIONS 408
UNDEFINING PERMISSIONS 410

MANAGING AUDIT, SHADOWING AND ALERTS FOR PROTOCOLS 411
DEFINING AND EDITING AUDIT AND SHADOWING RULES 426
ENABLING ALERTS 428
UNDEFINING AUDIT AND SHADOWING RULES 429

MANAGING PROTOCOLS WHITE LIST 430
DEFINING PROTOCOLS WHITE LIST 435
EDITING PROTOCOLS WHITE LIST 438
COPYING RULES OF PROTOCOLS WHITE LIST 439
EXPORTING AND IMPORTING PROTOCOLS WHITE LIST 440
UNDEFINING PROTOCOLS WHITE LIST 442
DELETING RULES OF PROTOCOLS WHITE LIST 443

MANAGING BASIC IP FIREWALL 444
DEFINING FIREWALL RULES 447
EDITING FIREWALL RULES 449
COPYING FIREWALL RULES 450
EXPORTING AND IMPORTING FIREWALL RULES 451
UNDEFINING FIREWALL RULES 453
DELETING FIREWALL RULES 454

MANAGING SECURITY SETTINGS FOR PROTOCOLS 455
DEFINING AND CHANGING SECURITY SETTINGS 456
UNDEFINING SECURITY SETTINGS 456

INSPECTION AND CONTROL OF SSL-ENCRYPTED TRAFFIC 457

DEVICELOCK REPORTS 459

REPORT CATEGORIES AND TYPES 459
AUDIT LOG REPORTS 460
SHADOW LOG REPORTS 471

CONFIGURING E-MAIL DELIVERY OF REPORTS 477
SETTING DEFAULT FORMAT FOR REPORTS 478
DEFINING REPORT PARAMETERS 479
REPORT OPTIONS DIALOG BOX 479
MANAGING REPORTS 487
RUNNING REPORTS 487
REFRESHING REPORTS 488
VIEWING REPORTS 489
VIEWING REPORT PARAMETERS 489
EXPORTING AND SAVING REPORTS 490
SENDING REPORTS THROUGH E-MAIL 491
DELETING REPORTS 491
DEVICELOCK SECURITY POLICIES (OFFLINE PROFILE) 493
CONFIGURING OFFLINE MODE DETECTION SETTINGS 494
SWITCHING BETWEEN ONLINE AND OFFLINE MODE 496
MANAGING OFFLINE SECURITY POLICIES FOR DEVICES 496
MANAGING OFFLINE PERMISSIONS 497
MANAGING OFFLINE AUDIT, SHADOWING AND ALERTS 501
MANAGING OFFLINE USB DEVICES WHITE LIST 507
MANAGING OFFLINE MEDIA WHITE LIST 514
MANAGING OFFLINE CONTENT-AWARE RULES FOR DEVICES 520
MANAGING OFFLINE SECURITY SETTINGS 531
MANAGING OFFLINE SECURITY POLICIES FOR PROTOCOLS 535
MANAGING OFFLINE PERMISSIONS FOR PROTOCOLS 536
MANAGING OFFLINE AUDIT, SHADOWING AND ALERTS FOR PROTOCOLS 540
MANAGING OFFLINE PROTOCOLS WHITE LIST 545
MANAGING OFFLINE IP FIREWALL 555
MANAGING OFFLINE CONTENT-AWARE RULES FOR PROTOCOLS 565
MANAGING OFFLINE SECURITY SETTINGS FOR PROTOCOLS 576
TEMPORARY WHITE LIST 579
TEMPORARY WHITE LIST AUTHORIZATION TOOL 580
APPENDIX 583
PERMISSIONS AND AUDIT EXAMPLES FOR DEVICES 583
PERMISSIONS EXAMPLES 583
AUDIT & SHADOWING RULES EXAMPLES 594
PERMISSIONS EXAMPLES FOR PROTOCOLS 596
CONTENT-AWARE RULES EXAMPLES 599
BASIC IP FIREWALL RULE EXAMPLES 603

About This Manual

This manual provides detailed information about how to install and use DeviceLock. It is primarily intended for administrators, security specialists, and other IT professionals who focus on how to provide data security within an organization.

This manual assumes some basic knowledge of the Microsoft Windows operating system and networking as well as the ability to create a local area network (LAN).

Conventions

The following table lists the conventions used in this manual.

CONVENTION	DESCRIPTION
Bold text	Represents user interface elements such as menus and commands, dialog box titles and options.
Italic text	Used for comments.
Blue text	Represents hyperlinks.
Note	Used to provide supplementary information.
Caution	Used to alert you to possible problems.
Best Practice	Used to provide best practice recommendations.
Plus sign (+)	Used to indicate a combination of keys that you must press at the same time.

Overview

General Information

Preventing unauthorized downloading as well as the uploading of inappropriate software and data is important when trying to protect and administer a company's computer network.

DeviceLock DLP Suite is easy to install. Administrators can have instant access from remote computers when necessary. The administrator of the machine or domain can designate user access to printers, clipboard, iPhones and iPads, floppy drives, optical drives, other removable media, tape drives, Media Transfer Protocol (MTP), WiFi, and Bluetooth adapters, or USB, FireWire, infrared, serial and parallel ports. All types of file systems are supported.

DeviceLock DLP Suite provides control over network communications. Administrators can designate user access to the FTP, HTTP, IBM Notes, SMB, SMTP, MAPI (Microsoft Exchange), Telnet and Torrent protocols, instant messengers (Skype, ICQ/AOL Instant Messenger, Windows Live Messenger and Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), cloud storages (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive, etc.), webmail, WhatsApp Web and social networking applications (AOL Mail, Gmail, GMX Mail, Hotmail (Outlook.com), Mail.ru, Outlook Web App (OWA), Rambler Mail, Web.de, Yahoo! Mail, and Yandex Mail; Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, StudiVZ, Tumblr, Twitter, Vkontakte, XING, Disqus, LiveInternet.ru).

DeviceLock extracts and filters the content of data copied to removable drives and plug-n-play storage devices, as well as that transmitted over the network. Administrators can create rules that specify which content can be copied and transmitted.

DeviceLock can audit user activity for a particular device type or protocol on a local computer. Based on the user's security context, this capability allows you to audit activities that belong to a certain user or user group. DeviceLock employs the standard event logging subsystem and writes audit records to the Windows event log.

DeviceLock can generate real-time security alerts when significant incidents, events or problems occur. Real-time alerting simplifies event monitoring and log management and helps you response faster and more efficiently to security incidents and policy violations. Alerts are available via Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).

DeviceLock supports data shadowing – the ability to mirror all data copied to external storage devices, transferred through serial and parallel ports or transmitted

over the network. A full copy of the files can be saved into the SQL database. Shadowing, like auditing, can be defined on a per-user basis.

Moreover, the DeviceLock data shadowing function is compatible with the National Software Reference Library maintained by the National Institute of Standards and Technology (NIST) and with the Hashkeeper Database designed and maintained by U.S. DOJ National Drug Intelligence Center (NDIC).

The data logged by DeviceLock can be checked against hash databases (collections of digital signatures of known, traceable data) and used in computer forensics.

You may also create your own database with digital signatures (SHA-1, MD5 and CRC32 are supported) of critical files and then use it for tracing purposes. For example, you can trace which users are copying signatured files, at what time, and with which devices.

For information on how to use hash databases in cooperation with DeviceLock, please contact our technical support team.

More information about hash databases and their samples can be found at the National Software Reference Library's Web site: http://www.nsrl.nist.gov.

Also, DeviceLock provides instant searching of text across shadowed files and audit logs stored in the centralized database. DeviceLock can automatically recognize, index, search and display documents in many formats, such as: Adobe Acrobat (including encrypted files if the type of encryption in the file is one of the following: 40-bit RC4, 128-bit RC4, 128-bit AES and 256-bit AES, and the file permissions do not disable text extraction) (PDF), Ami Pro, AutoCAD (DWG, DXF), Archives (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (documents, spreadsheets and presentations), Quattro Pro, WordPerfect, WordStar and many others.

Note: Content in AutoCAD (DWG, DXF) file formats can be identified on Windows XP and later systems.

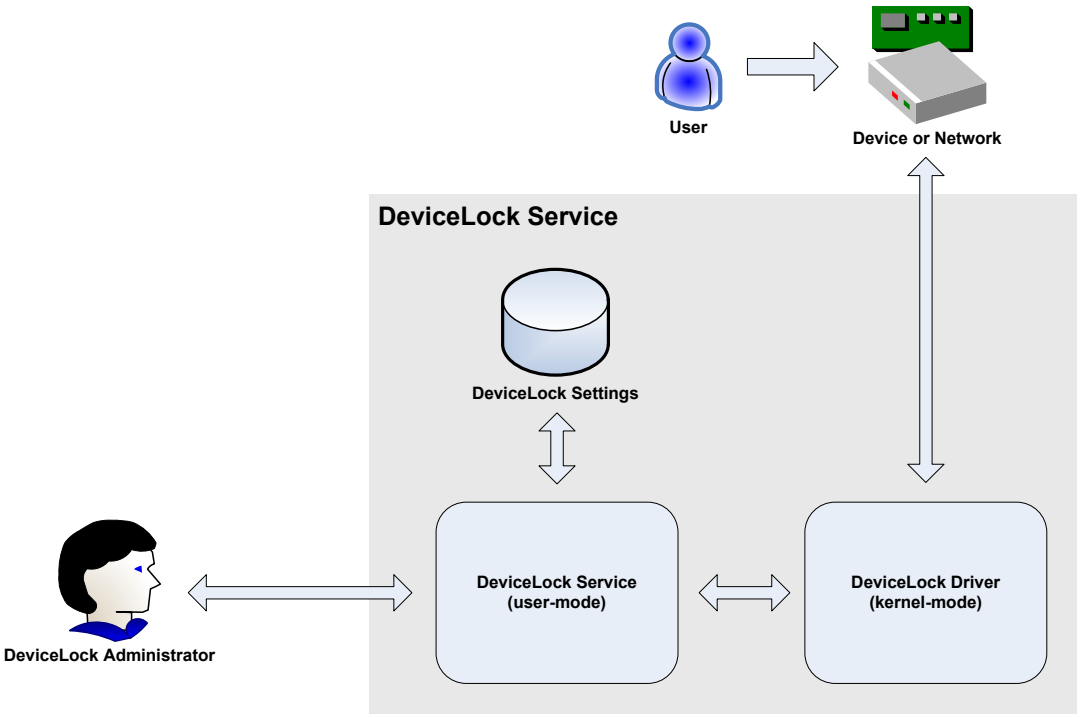
In addition to the standard (per computer) way of managing permissions, DeviceLock also provides you with a more powerful mechanism – permissions and settings can be changed and deployed via Group Policy in an Active Directory domain.

Tighter integration into the Active Directory is a very important function of DeviceLock. It makes DeviceLock's permissions management and deployment easier for large networks and more convenient for system administrators.

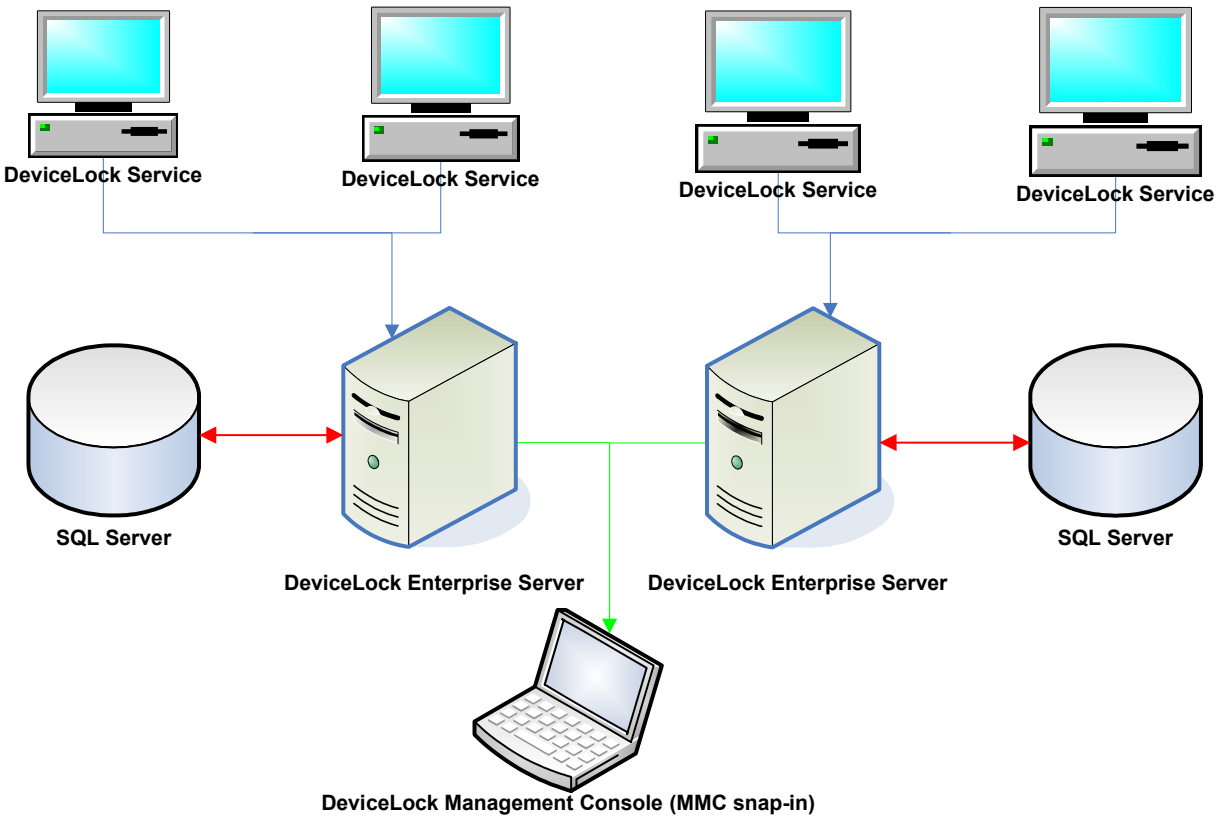
Integration into the Active Directory eliminates the need to install more third-party applications for centralized management and deployment. DeviceLock does not need to have its own server-based version to control the entire network, instead it uses standard functions provided by the Active Directory.

DeviceLock DLP Suite consists of three parts: the agent (DeviceLock Service), the server (DeviceLock Enterprise Server and DeviceLock Content Security Server) and the management console (DeviceLock Management Console, DeviceLock Group Policy Manager, DeviceLock WebConsole and DeviceLock Enterprise Manager).

1. DeviceLock Service is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device and network protection on the client machine while remaining invisible to that computer's local users.

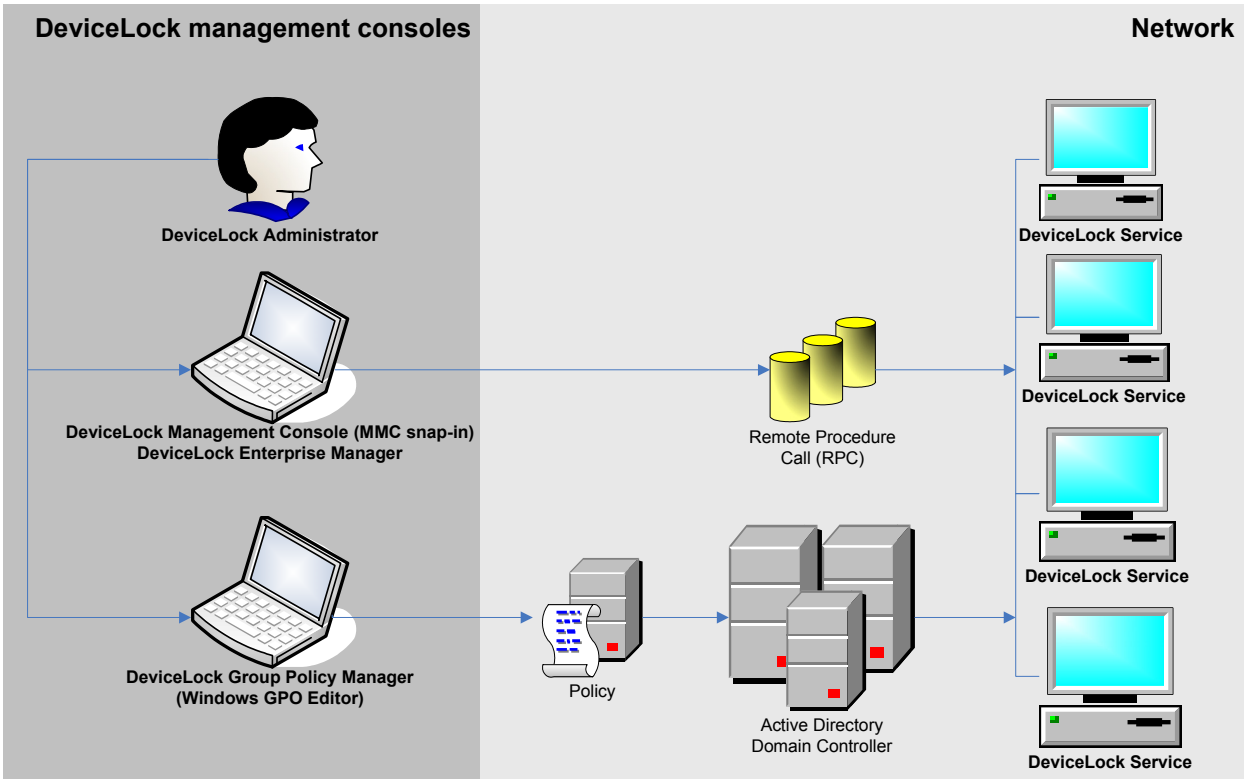


2. DeviceLock Enterprise Server is an optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock Enterprise Server uses MS SQL Server to store its data. You can install several DeviceLock Enterprise Servers to uniformly spread the network load.



DeviceLock Content Security Server is another optional component which includes Search Server for instant search of text within shadowed files and other logs stored on DeviceLock Enterprise Server. For more information, see "Understanding DeviceLock Content Security Server."

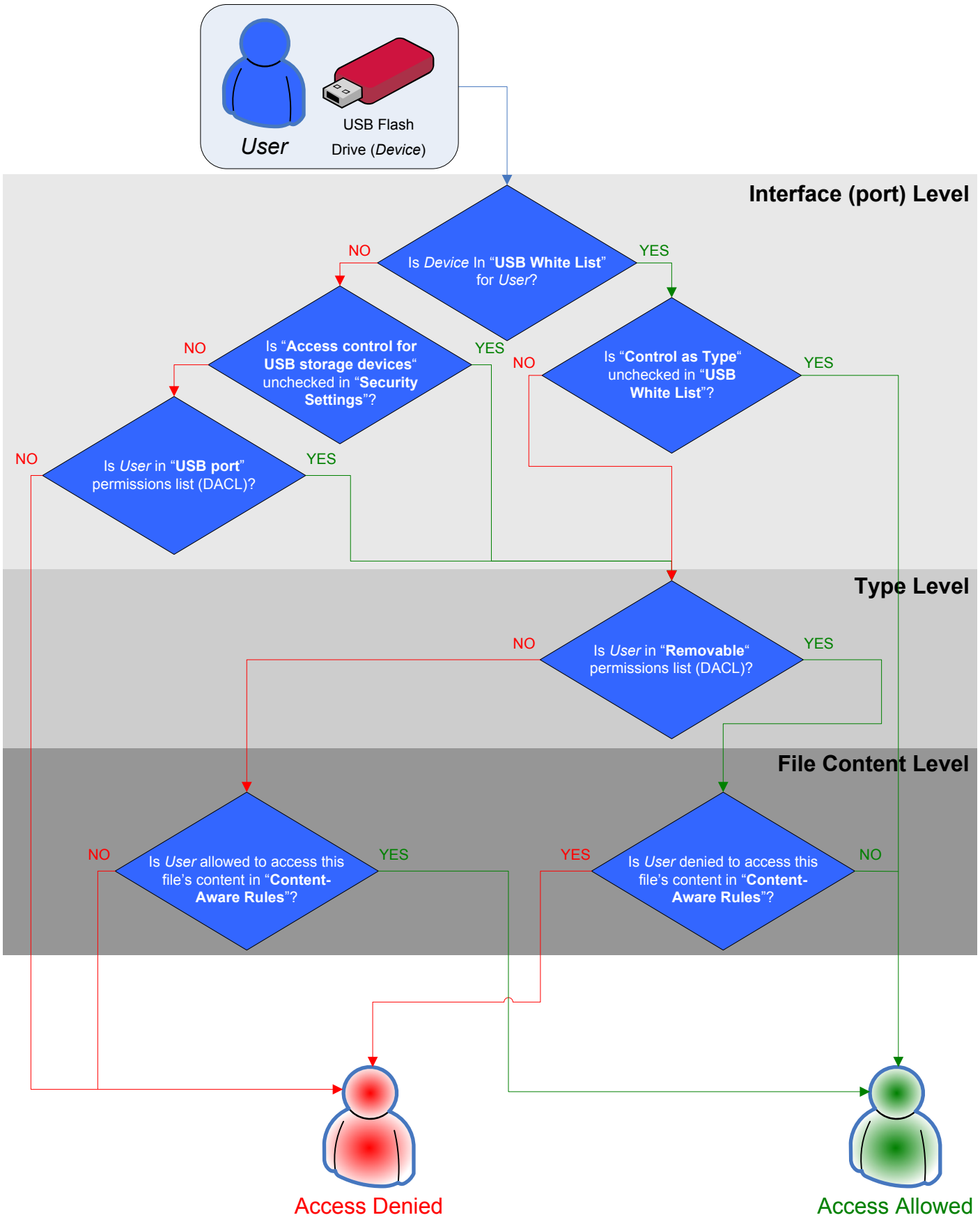
3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with four different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager, DeviceLock WebConsole and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor). DeviceLock Management Console and DeviceLock WebConsole are also used to manage DeviceLock Enterprise Server and DeviceLock Content Security Server.



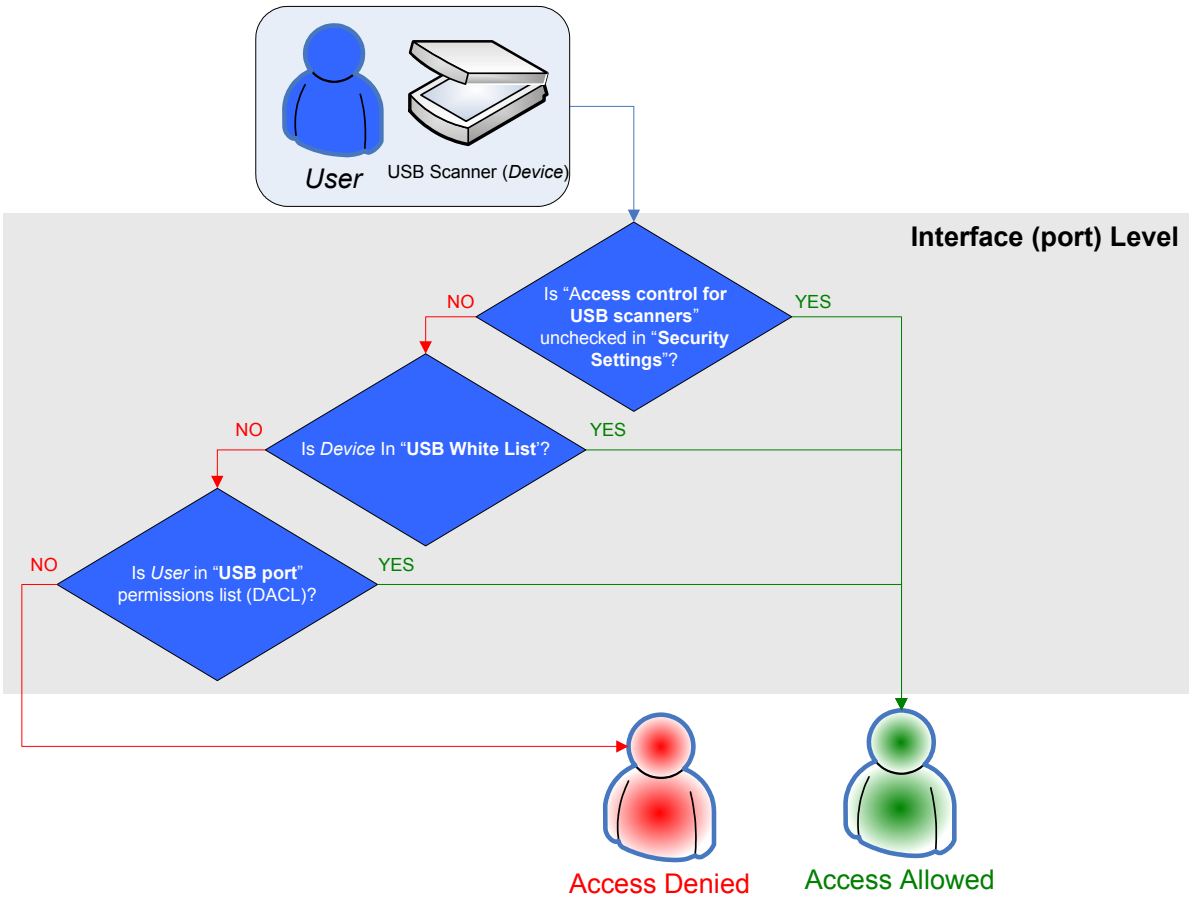
Managed Access Control for Devices and Protocols

Access control for devices works in the following way: Every time the user wants to access a device, DeviceLock intercepts this request at the kernel level of the OS. Depending on the device's type and the connection interface (e.g. USB), DeviceLock checks the user rights in the appropriate Access Control List (ACL). If the user does not have the right to access this device, an "access denied" error is returned.

Access checking can occur at three levels: the interface (port) level, the type level and the file content level. Some devices are checked at all three levels, while others only at one level – either interface (port) or type.


User
USB Flash Drive (*Device*)
Interface (port) Level
Is *Device* In "**USB White List**" for *User*?
NO
YES
Is "**Access control for USB storage devices**" unchecked in "**Security Settings**"?
NO
YES
Is "**Control as Type**" unchecked in "**USB White List**"?
NO
YES
Is *User* in "**USB port**" permissions list (DACL)?
NO
YES
Type Level
Is *User* in "**Removable**" permissions list (DACL)?
NO
YES
File Content Level
Is *User* allowed to access this file's content in "**Content-Aware Rules**"?
NO
YES
Is *User* denied to access this file's content in "**Content-Aware Rules**"?
YES
NO
Access Denied
Access Allowed

Consider the case of a user connecting a USB flash drive to the USB port. Here DeviceLock would first check whether the USB port is open or locked at the interface level. Next, because Windows recognizes a USB flash drive as a removable storage device, DeviceLock will also check permissions at the type level (Removable). Finally, DeviceLock will also check permissions at the file content level (Content-Aware Rules). In contrast, a USB scanner would only be checked at the interface level (USB port), as DeviceLock doesn't distinguish scanners at the type level.



There are additional Security Settings that can turn off access control for classes of devices (for example, all USB printers) while others remain under control. In the case of a device belonging to a class for which control is disabled, DeviceLock allows all requests to connect this device at the interface (port) level.

Also, DeviceLock supports the white listing of specific devices; in other words, you can turn off access control for only specific devices (for example, certain USB printer).

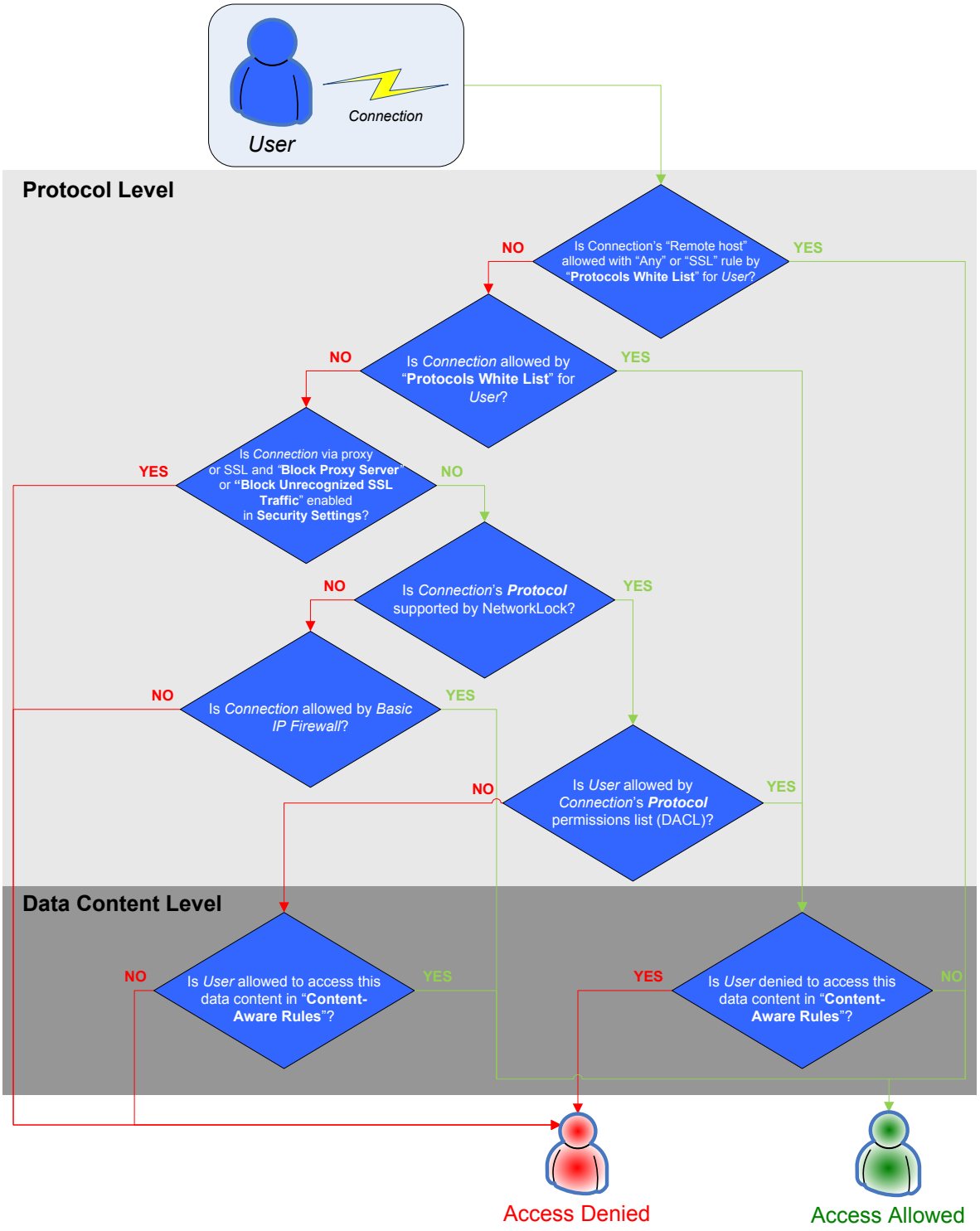
Note: If access to a device is denied at the interface (port) level, DeviceLock does not check permissions at the type level. However, if access is granted at the interface (port) level, DeviceLock also checks permissions at the type level. Only when access is granted at both levels, the user can connect the device.

Access control for protocols works in the following way: Every time the user wants to access a remote network resource, DeviceLock intercepts this connection request at the kernel level of the OS and checks the user rights in the appropriate Access Control List (ACL). If the user does not have the right to access this protocol, an "access denied" error is returned.

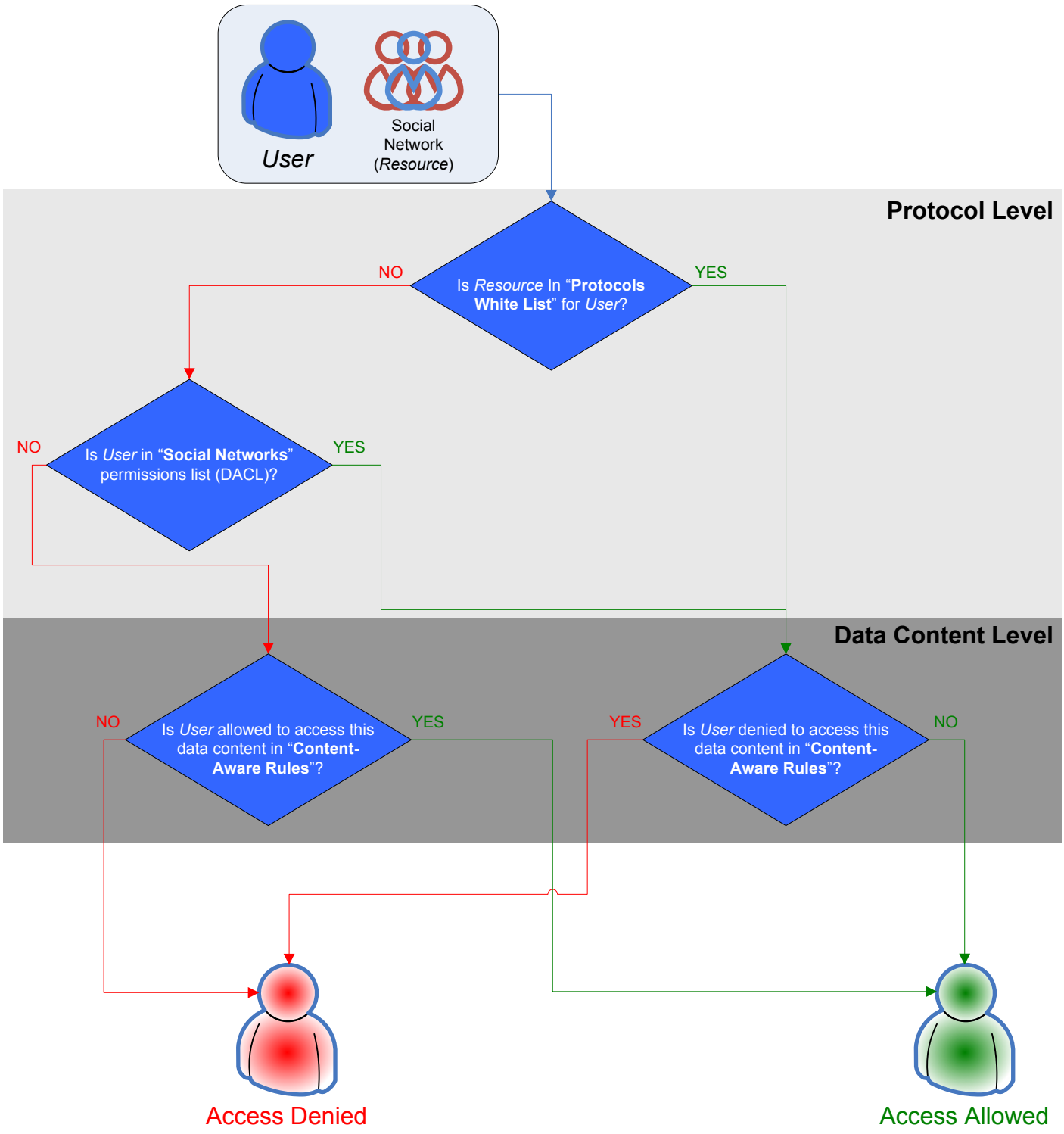
Note: Access control settings for Social Networks, File Sharing and Web Mail override access control settings for HTTP. For example, if users are allowed to access Gmail, but disallowed to use HTTP, they nevertheless can access the service.

Access checking can occur at two levels: the protocol level and the data content level. All network connections except for Telnet and Torrent connections are checked at both levels.

For example, consider the case when a user attempts to connect to a remote host. Here DeviceLock would first check whether the user is allowed to access the connection at the protocol level. Next, DeviceLock will also check permissions at the data content level (Content-Aware Rules).



For another example, consider the case of a user connecting to a social networking site. Here DeviceLock would first check whether Social Networks are open or locked at the protocol level. Next, DeviceLock will also check permissions at the data content level (Content-Aware Rules).



Also, DeviceLock supports the white listing of protocols. With the Protocols White List, you can turn off access control for connections with specific parameters (for example, HTTP connections to specific hosts and ports).

DeviceLock Service for Mac

DeviceLock Service for Mac is designed to help network administrators prevent unauthorized data transfers, block file copying and prevent software uploads and downloads.

Supporting a wide range of storage protocols, media and devices, DeviceLock Service for Mac provides highly customizable and flexible access control to internal and external storage devices such CD, DVD, BD burners, external disks, floppy drives, USB drives and pen-drives; controls access to WiFi and Bluetooth adapters, and provides managed access to, USB, FireWire, and serial ports. eSATA hardware can be controlled as Removable devices, while Thunderbolt devices can be controlled as Removable and WiFi hardware.

DeviceLock Service for Mac includes the following features:

- **Access Control for Ports and Storage Devices**. With DeviceLock Service for Mac, network administrators gain full control over who, when, and under what conditions can gain access to certain devices, ports. This helps prevent data leaks including unauthorized software installations.
- **Audits User Activities**. DeviceLock Service for Mac can audit user activity for a particular device type on a local computer. Based on the user's security context, this capability allows administrators to audit activities that belong to a certain user or user group. The tool can create log files collected by DeviceLock Enterprise Server and displayed by management consoles.
- **Data Shadowing**. DeviceLock Service for Mac enables administrators to see what information exactly has been transferred by creating a shadow copy of all data sent or received via certain ports, devices. The system uses data shadowing to mirror all data copied to external storage devices. A full copy of files being transferred can be saved into a SQL database. Shadowing, like auditing, can be defined on per-user basis.
- **Active Directory Integration**. Tight integration into the Active Directory makes DeviceLock Service for Mac easier to configure and manage, simplifies permission management and maintenance in large heterogeneous networks. Integrating DeviceLock Service for Mac into a network domain allows retrieving configuration settings from Active Directory via DeviceLock Enterprise Server.

Understanding DeviceLock Content Security Server

DeviceLock Content Security Server is an optional component of DeviceLock DLP Suite. It includes Search Server which provides full-text searching of logged data stored on DeviceLock Enterprise Server, and Discovery Server used to discover certain types of content existing on the computers and storage devices connected to the local network. The search capabilities of Search Server make it easier and more efficient to manage the increasing amount of data in DeviceLock Enterprise Server databases. Discovery Server, in its turn, is the component of DeviceLock Discovery product, that can be used separately from-, or as a part of DeviceLock DLP Suite. Further information on Discovery Server is available in DeviceLock Discovery User Manual. This manual only includes information on Search Server.

DeviceLock Content Security Server includes the following features:

- **Full-text search capability support**. Through the use of Search Server, DeviceLock Content Security Server allows you to instantly search for relevant text data based on various search criteria.
- **Flexible configuration options**. There is support for many different configuration options, enabling you to optimize the performance of DeviceLock Content Security Server for your unique installation.

You can use full-text searches to find data that you cannot find by filtering data in the log viewers. The full-text search functionality is especially useful in situations when you need to search for shadow copies of documents based on their contents.

Use Case – Preventing leaks of confidential information
Security specialists who are tasked with keeping sensitive information confidential can regularly use Search Server to easily find, retrieve and analyze all shadow copies of files containing specific business-critical data, for example, customers or price lists. The log records associated with found shadow copies will help to determine when and by whom confidential information was copied. With this information, security specialists can take immediate steps to avoid possible information disclosure and distribution outside the company.

You can configure and use DeviceLock Content Security Server by using DeviceLock Management Console.

How Search Server Works

Search Server performs the following functions:

- Indexes DeviceLock Enterprise Server data.
- Executes full-text queries after the data has been indexed.

These functions are described in more detail below.

Indexing DeviceLock Enterprise Server Data

Indexing is a process through which the textual data on DeviceLock Enterprise Server becomes searchable and retrievable.

Search Server starts the indexing process automatically as soon as you specify DeviceLock Enterprise Server(s). The indexing process can result in either the creation or update of the full-text index. There is only one full-text index per Search Server, making management more efficient. The full-text index stores information about significant words and their location. During index creation or update, Search Server discards noise words (such as prepositions, articles, and so on) that do not help the search.

Search Server indexes all text data from the following content sources: Audit Log, Shadow Log, Deleted Shadow Data Log, Server Log, and Monitoring Log.

The indexing process happens in two stages. In the first stage, Search Server extracts significant words from shadow copies and log records and saves them to temporary indexes for each specified DeviceLock Enterprise Server. For each temporary index, Search Server processes 1,000 records from each log. In the second stage, when either the number of temporary indexes becomes equal to 50 or 10 minutes pass, all temporary indexes are combined into a permanent master index that is used for search queries. The process of combining temporary indexes into a master index is called ***merging***.

The creation of the master index is a time-intensive process. Indexing speed can vary considerably depending on the type of data being indexed and the hardware being used. Generally, indexing speed is between 30 and 120 MB/minute. Consider the following example:

- Data: 170 GB, consisting of 4,373,004 mixed-type files (HTML, office documents, text)
- Indexing time: 24.7 hours (6.8 GB/hour)
- Index size: 12% of original document size
- Hardware: Pentium® 4 Processor 550 (3.40GHz, 800 FSB), 2GB RAM, internal SATA RAID-0 drives

Executing Full-Text Queries

After the DeviceLock Enterprise Server data has been indexed, you can run full-text queries. These queries can search for one or more specific words or phrases. When a search query is executed, Search Server processes the query and retrieves a list of results from the index that matches the criteria of the query. Filtering can be applied to the search to narrow the result set returned. For example, the results can be filtered by log or date. Querying the full-text index is extremely fast and flexible. A search operation takes only seconds to locate and return matches for particular

search criteria. For detailed information about the search results page and search results, see "Working with Search Results."

Extending DeviceLock Functionality with ContentLock and NetworkLock

DeviceLock DLP Suite comes with ContentLock and NetworkLock – separately licensed components that provide additional functionality for DeviceLock. These components are installed automatically but require a license to function. For more information on ContentLock and NetworkLock licenses, see "Licensing."

Note: ContentLock and NetworkLock are not yet supported in DeviceLock Service for Mac.

NetworkLock adds comprehensive context control capabilities over endpoint network communications. It supports port-independent network protocol and application detection and selective blocking, message and session reconstruction with file, data, and parameter extraction, as well as event logging and data shadowing. NetworkLock controls most popular network protocols and applications such as: plain and SSL-protected SMTP email communications (with messages and attachments controlled separately), communications between the Microsoft Outlook client and Microsoft Exchange Server (the MAPI protocol), IBM Notes, Web access and other HTTP-based applications including content inspection of encrypted HTTPS sessions (specifically, webmail, WhatsApp Web and social networking applications like Gmail, Yahoo! Mail, Windows Live Mail, Facebook, Twitter, LiveJournal, etc.), instant messengers (Skype, ICQ/AOL Instant Messenger, Windows Live Messenger and Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), cloud storages (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive, etc.), file transfers over FTP and FTP-SSL protocols, local network files transfers over SMB, as well as telnet and torrent sessions.

NetworkLock is represented in the user interface of DeviceLock Management Console, Service Settings Editor and DeviceLock Group Policy Manager by the **Protocols** node.

NetworkLock includes the following key features and benefits:

- **Protocol access control**. You can control which users or groups can gain access to the FTP, HTTP, IBM Notes, SMTP, MAPI (Microsoft Exchange), SMB, Telnet and Torrent protocols, instant messengers (Skype, ICQ/AOL Instant Messenger, Windows Live Messenger and Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), cloud storages (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive, etc.), as well as webmail, WhatsApp Web

and social networking applications (AOL Mail, Gmail, GMX Mail, Hotmail (Outlook.com), Mail.ru, Outlook Web App (OWA), Rambler Mail, Web.de, Yahoo! Mail, Yandex Mail; Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, StudiVZ, Tumblr, Twitter, Vkontakte, XING, Disqus, LiveInternet.ru) depending on the time of day and day of the week.

- **Protocols White List**. Lets you selectively allow network communication over specified protocols regardless of existing protocol blocking settings. The white list is most effective in "least privilege" scenarios when you block all protocol traffic and then specifically authorize only what is required for employees to perform their daily job duties.
- **Content-Aware Rules (File Type Detection)**. You can selectively allow or deny access to specific types of files transmitted over the network. Recognition and identification of file types is based solely upon the content of files. This efficient and reliable algorithm allows for correct identification and handling of files regardless of the file extension. You can also use Content-Aware Rules to allow or deny shadow copying of specific file types.

  Note: You must purchase a ContentLock license to gain access to enhanced capabilities of the Content-Aware Rules feature.

- **Audit, shadowing and alerts**. Allows you to track user activity for specified protocols and log a full copy of data/files transmitted over the network.

ContentLock is a content monitoring and filtering component that greatly enhances the capabilities of the Content-Aware Rules feature. With ContentLock, you can not only grant or deny access to information based on real file types but also create regular expressions patterns with numerical conditions and Boolean combinations of matching criteria and keywords. Recognizing more than eighty file formats and data types, ContentLock extracts and filters the content of data copied to removable drives and plug-n-play storage devices, as well as that transmitted over the network. With ContentLock, you can also filter shadowed data down to just those pieces of information meaningful to security auditing, incident investigations and forensic analysis before saving in the Shadow Log. This tremendously reduces storage space and network bandwidth requirements for shadow log delivery to the central database.

ContentLock includes the following key features and benefits:

- **Content-based document access control**. You can control access to documents depending on their content. Thus, you can block sensitive content leakage while allowing authorized employees to gain access to the information they need to collaborate.

- **Oracle IRM support**. You can control access to documents that have been sealed using Oracle Information Rights Management (IRM).
- **Content-based filtering of shadow data**. You can specify that only data that contains sensitive information is shadow copied and saved to the Shadow Log, thus reducing the volume of unnecessary log data and making the log files easier to work with.
- **Expansive coverage of multiple file formats and data types**. You can analyze content of the following file formats and data types: Adobe Acrobat (including encrypted files if the type of encryption in the file is one of the following: 40-bit RC4, 128-bit RC4, 128-bit AES and 256-bit AES, and the file permissions do not disable text extraction) (*.pdf), Adobe Framemaker MIF (*.mif), Ami Pro (*.sam), Ansi Text (*.txt), ASCII Text, ASF media files (metadata only) (*.asf), AutoCAD (*.dwg, *.dxf), CSV (Comma-separated values) (*.csv), DBF (*.dbf), EBCDIC, EML (emails saved by Outlook Express) (*.eml), Enhanced Metafile Format (*.emf), Eudora MBX message files (*.mbx), Flash (*.swf), GZIP (*.gz), HTML (*.htm, *.html), iCalendar (*.ics), Ichitaro (versions 5 and later) (*.jtd, *.jbw), JPEG (*.jpg), Lotus 1-2-3 (*.123, *.wk?), MBOX email archives such as Thunderbird (*.mbx), MHT archives (HTML archives saved by Internet Explorer) (*.mht), MIME messages (including attachments), MSG (emails saved by Outlook) (*.msg), Microsoft Access MDB files (*.mdb, *.accdb, including Access 2007 and Access 2010), Microsoft Document Imaging (*.mdi), Microsoft Excel (*.xls), Microsoft Excel 2003 XML (*.xml), Microsoft Excel 2007, 2010, and 2013 (*.xlsx), Microsoft OneNote 2007, 2010, and 2013 (*.one), Microsoft Outlook data files (*.PST), Microsoft Outlook/Exchange Messages, Notes, Contacts, Appointments, and Tasks, Microsoft Outlook Express 5 and 6 (*.dbx) message stores, Microsoft PowerPoint (*.ppt), Microsoft PowerPoint 2007, 2010, and 2013 (*.pptx), Microsoft Rich Text Format (*.rtf), Microsoft Searchable Tiff (*.tiff), Microsoft Word for DOS (*.doc), Microsoft Word for Windows (*.doc), Microsoft Word 2003 XML (*.xml), Microsoft Word 2007, 2010, and 2013 (*.docx), Microsoft Works (*.wks), MP3 (metadata only) (*.mp3), Multimate Advantage II (*.dox), Multimate version 4 (*.doc), OpenOffice versions 1, 2, and 3 documents, spreadsheets, and presentations (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (includes OASIS Open Document Format for Office Applications), Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw), QuickTime (*.mov, *.m4a, *.m4v), RAR (*.rar), TAR (*.tar), TIFF (metadata only) (*.tif), TNEF (winmail.dat), Treepad HJT files (*.hjt), Unicode (UCS16, Mac or Windows byte order, or UTF-8), Visio XML files (*.vdx), Windows Metafile Format (*.wmf), WMA media files (metadata only) (*.wma), WMV video files (metadata only) (*.wmv), WordPerfect 4.2 (*.wpd, *.wpf), WordPerfect (5.0 and later) (*.wpd, *.wpf), WordStar version 1, 2, 3 (*.ws), WordStar versions 4, 5, 6 (*.ws), WordStar 2000, Write (*.wri), XBase (including FoxPro, dBase, and other XBase-compatible formats) (*.dbf), XML (*.xml), XML Paper

Specification (*.xps), XSL, XyWrite, ZIP (*.zip) as well as PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, EMF spooled files and GDI printing (ZjStream).

Note: The content of AutoCAD (DWG, DXF) file formats can be analyzed on Windows XP and later systems.

- **Automated protection of new documents**. You can automatically apply content-based security policies to new documents as they are created.
- **Multiple content detection methods**. You can use multiple methods to identify sensitive content contained in documents (based on regular expressions, keywords, and document properties).
- **Centralized content management**. Content-Aware Rules are created based on content groups that enable you to centrally define types of content for which you want to control access.
- **Ability to override device type/protocol–level policies**. You can selectively allow or deny access to certain content regardless of preset permissions at the device type-/protocol-level.
- **Inspection of files within archives**. Allows you to perform deep inspection of each individual file contained in an archive. The following inspection algorithm is used: When a user attempts to copy an archive file to a device or transmit it over the network, all files are extracted from the archive and analyzed separately to detect the content to which access is denied by Content-Aware Rules. If Content-Aware Rules deny access to at least one of the files extracted from the archive, the user is denied access to the archive. If Content-Aware Rules allow access to all of the files extracted from the archive, the user is allowed access to the archive. All archived files are extracted to the Temp folder of the System user. Typically, the system Temp folder resides in the following location: %windir%\Temp directory. If DeviceLock Service has no access to the Temp folder, the archived files are not analyzed and access to the archive is denied only if any one of the following conditions is true:
    - There is a Deny Content-Aware Rule
    - Permissions set for the device type or protocol deny access

  All nested archives are also unpacked and analyzed one by one. Archive files are detected by content, not by extension. The following archive formats are supported: 7z (.7z), ZIP (.zip), GZIP (.gz, .gzip, .tgz), BZIP2 (.bz2, .bzip2, .tbz2, .tbz), TAR (.tar), RAR (.rar), CAB (.cab), ARJ (.arj), Z (.z, .taz), CPIO (.cpio), RPM (.rpm), DEB (.deb), LZH (.lzh, .lha), CHM (.chm, .chw, .hxs), ISO (.Iso), UDF (.Iso), COMPOUND (.Msi), WIM (.wim, .swm), DMG (.dmg), XAR (.xar), HFS (.hfs), NSIS (.exe), XZ (.xz), MsLZ (.mslz), VHD (.vhd), FLV (.flv), SWF (.swf) as well as CramFS, SquashFS (.squashfs), NTFS, FAT, and MBR file system and disk images. Split (or multi-volume) and password-protected archives are not unpacked.

Note: To allow transfer of split (or multi-volume) archives in case there are active content-aware rules combined with **Archives content inspection on read** or **Archives content inspection on write** options enabled in **Service options**, create an allow content aware **Document Properties** rule with the **Text extraction not supported** flag checked.

- **Optical Character Recognition (OCR)**. The use of the OCR technology allows you to extract text from images (such as scanned documents, screen shots, etc.) for further content analysis by Content-Aware Rules. The built-in OCR supports the following languages: Bulgarian, Catalan, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Hungarian, Indonesian, Italian, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, and Turkish. The following image files are supported for OCR processing: BMP files, Dr. Halo CUT files, DDS files, EXR files, Raw Fax G3 files, GIF files, HDR files, ICO files, IFF files (except Maya IFF files), JBIG files, JNG files, JPEG/JIF files, JPEG-2000 files, JPEG-2000 codestream files, KOALA files, Kodak PhotoCD files, MNG files, PCX files, PBM/PGM/PPM files, PFM files, PNG files, Macintosh PICT files, Photoshop PSD files, RAW camera files, Sun RAS files, SGI files, TARGA files, TIFF files, WBMP files, XBM files, and XPM files.

  Note: You must install "Update Rollup 1 for Windows 2000 SP4 (KB891861)" http://www.microsoft.com/en-us/download/details.aspx?id=18997 to use OCR technology on computers running Windows 2000 operating system.

- **Text in picture detection**. The use of the text in picture detection technology allows you to classify all images into two groups: text images (images that contain text, for example, scanned documents, screen shots of documents) and non-text images (images that do not contain text) and separately control access to each group. For example, you can allow certain users to copy non-text images to devices, but prevent them from writing text images thus preventing leakage of sensitive information within image files. The following image files are supported: BMP files, Dr. Halo CUT files, DDS files, EXR files, Raw Fax G3 files, GIF files, HDR files, ICO files, IFF files (except Maya IFF files), JBIG files, JNG files, JPEG/JIF files, JPEG-2000 files, JPEG-2000 codestream files, KOALA files, Kodak PhotoCD files, MNG files, PCX files, PBM/PGM/PPM files, PFM files, PNG files, Macintosh PICT files, Photoshop PSD files, RAW camera files, Sun RAS files, SGI files, TARGA files, TIFF files, WBMP files, XBM files, and XPM files.
- **Inspection of images embedded in documents**. Allows you to perform deep inspection of each individual image embedded in saved emails (EML), Adobe Portable Document Format (including encrypted files if the type of encryption in the file is one of the following: 40-bit RC4, 128-bit RC4, 128-bit AES and 256-bit AES, and the file permissions do not disable text extraction) (PDF) files, Rich Text Format (RTF), AutoCAD files (.dwg, .dxf), and Microsoft Office documents (.doc, .xls, .ppt, .docx, .xlsx, .pptx). All embedded images are extracted from these documents to the Temp folder of the System user

and analyzed independently from text to detect the content to which access is denied by Content-Aware Rules. The text contained inside documents is checked by Content-Aware Rules that are created based on Keywords, Pattern or Complex content groups. Embedded images are checked by Content-Aware Rules that are created based on Keywords, Pattern, File Type Detection, Document Properties or Complex content groups. Access to documents is granted only when Content-Aware Rules allow access to text and all of the images contained in documents.

Note: Deep inspection of images embedded in files of AutoCAD (DWG, DXF) formats can be performed on Windows XP and later systems only.

Licensing

If you want to use the capabilities of NetworkLock and ContentLock, you must purchase NetworkLock and ContentLock licenses in addition to basic DeviceLock licenses.

A NetworkLock license enables you to use the Protocols feature.

A ContentLock license enables you to create and use Content-Aware Rules based on regular expressions, keywords, and document properties as well as complex rules based on Boolean combinations of matching criteria.

If you use different types of licenses, consider the following:

- If you have a basic DeviceLock license, a ContentLock license, and a NetworkLock license, you can use the Protocols feature, create and use Content-Aware Rules based on file types, regular expressions, keywords, and document properties as well as complex rules.
- If you have only a basic DeviceLock license, you cannot use the Protocols feature, and you cannot create and use Content-Aware Rules based on regular expressions, keywords, and document properties as well as complex rules. You can create and use Content-Aware Rules based on file types (File Type Detection).
- If you have a basic DeviceLock license and a ContentLock license, you can create and use Content-Aware Rules based on file types, regular expressions, keywords, and document properties as well as complex rules. You cannot use the Protocols feature.
- If you have a basic DeviceLock license and NetworkLock license, you can use the Protocols feature and create and use Content-Aware Rules based on file types. You cannot create and use Content-Aware Rules based on regular expressions, keywords, and document properties as well as complex rules.

- A basic DeviceLock license is obligatory, while NetworkLock and ContentLock licenses are optional. If a basic license is missing or invalid, DeviceLock runs in a trial mode only. The number of NetworkLock and/or ContentLock licenses must equal or exceed the number of basic DeviceLock licenses.
- The trial period for ContentLock and NetworkLock is 30 days.

Recommended Basic Security Measures

Following is a series of basic security rules that should be met for computers that you want to install in a corporate network:

- ***Change the boot sequence***. The hard disk must be the first boot device. Change the boot sequence in the BIOS so that the computer does not boot from the floppy, USB drive or CD-ROM. If the hard disk is not the first boot device, someone can use a bootable CD or USB Flash Drive to directly access the hard disk drive.
- ***Protect the BIOS with a password***. The password should be set to the BIOS so only an authorized person can make changes there. If the BIOS is not password protected, someone can change the boot sequence and use a bootable CD, floppy or USB Flash Drive (see above).
- ***Seal computer cases and chassis***. Protect the hardware with a seal. Otherwise, it is possible to plug an external boot device directly to the computer and access the hard disk. Moreover, if someone can physically access the motherboard, it is very easy to locate the CMOS reset jumper and clear the BIOS password (see above).
- ***Do not give Administrative rights to regular users***. Regular local users should not be members of the local Administrators group. It is not a good practice to grant users administrative rights to their computers.

  However, if for some reason users on your network have administrator privileges on their local computers, DeviceLock provides another level of protection. No one except authorized DeviceLock administrators can connect to, stop, or uninstall DeviceLock Service. Even members of the local Administrators group cannot disable DeviceLock if they are not in the list of the authorized DeviceLock administrators.
- ***Remove the Recovery Console***. If the Windows Recovery Console is installed on the local computer, someone can boot to the recovery mode and workaround any number of security measures including disabling DeviceLock Service (however, this requires the local administrator password). For this reason, we recommend deleting the Recovery Console. For more information on how to install, remove and use the Recovery Console, please refer to the Microsoft's on-line article: https://support.microsoft.com/en-us/kb/307654.

Installation

Requirements

DeviceLock DLP Suite consists of three parts: the agent (DeviceLock Service), the server (DeviceLock Enterprise Server and DeviceLock Content Security Server) and the management console (DeviceLock Management Console, DeviceLock Group Policy Manager, DeviceLock WebConsole and DeviceLock Enterprise Manager).

Below you can find the system requirements for each part of DeviceLock DLP Suite.

The computer on which you install DeviceLock Service must meet the following system requirements:

Operating System for DeviceLock Service for Windows	Microsoft Windows NT 4.0 SP6/2000/XP/Vista/7/8/8.1/10 and Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2. Installation is supported on both the 32-bit and the 64-bit editions of the operating system. **Note:** Windows Internet Explorer version 4.0 or later must be installed on computers running Windows NT 4.0 SP 6.
Operating System for DeviceLock Service for Mac	Apple OS X 10.6.8 (Snow Leopard), 10.7 (Lion), 10.8 (Mountain Lion), 10.9 (Mavericks), 10.10 (Yosemite), 10.11 (El Capitan). Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
RAM	Minimum: 512 MB.
Hard Disk Space	Minimum: 400 MB.
Processor Type	Minimum: Intel Pentium 4.
Supported Virtualization Products	Microsoft Remote Desktop Services (RDS), Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View, VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC.

The computer on which you install DeviceLock management consoles must meet the following system requirements:

Operating System	Microsoft Windows 2000/XP/Vista/7/8/8.1/10 and Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2. Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
RAM	Minimum: 512 MB.

Hard Disk Space	Minimum: 1 GB.
Processor Type	Minimum: Intel Pentium 4.

The computer on which you install DeviceLock Enterprise Server and DeviceLock Content Security Server must meet the following system requirements:

Operating System	Microsoft Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2. Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
RAM	Minimum: 1024 MB. Recommended: 8 GB.
Hard Disk Space	Minimum:1 GB. Recommended: 800 GB (if an SQL database is used).
Processor Type	Minimum: Intel Pentium 4. Recommended: 2x Intel Xeon Quad Core 2.33 GHz.
Relational Database Management Systems	Microsoft SQL Server Data Engine (MSDE), SQL Server Express, SQL Server

To install and use DeviceLock, you MUST have administrative privileges. If you are going to use DeviceLock only on a local computer, you must have local administrative privileges. If you are going to use DeviceLock throughout your network, you must have domain administrator privileges.

If you want to use DeviceLock on your network, you must have a functioning TCP/IP network protocol. However, DeviceLock can also work on stand-alone computers. A network is needed only if you want to control DeviceLock Service from a remote computer.

The following TCP/UDP ports should be opened to allow communications between the DeviceLock Service, DeviceLock Enterprise Server, and DeviceLock Content Security Server services.

- 135 (TCP) - for Remote Procedure Call (RPC) Service;
- 137 (UDP) - for NetBIOS Name Service;
- 138 (UDP) - for NetBIOS Netlogon and Browsing;
- 139 (TCP) - for NetBIOS session (NET USE).

Additionally, these services, which are not running by default in Windows 8 and later systems, must be changed:

- **Remote Registry Service**

The startup type of the service must be set to Automatic.

- **Remote Procedure Call (RPC) Service**
  The startup type of the service must be set to Automatic.
- **Base Filtering Engine Service**
  The startup type of the service must be set to Automatic.

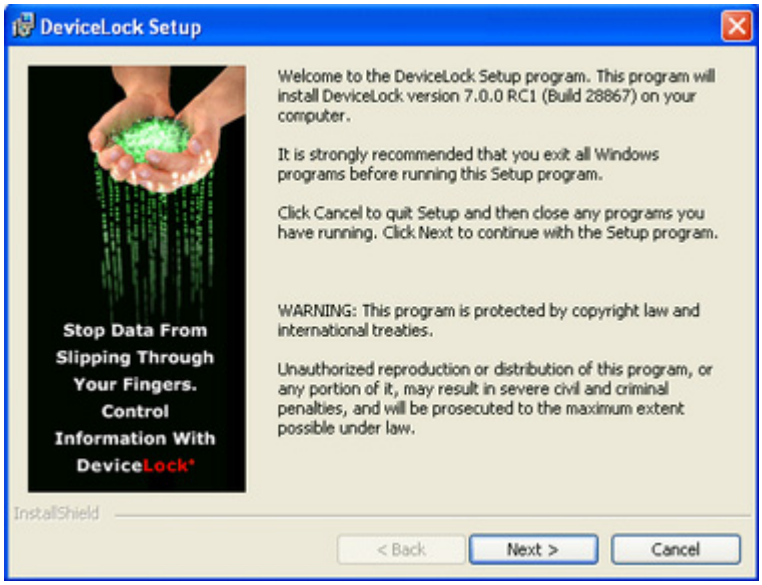
Note: Only applies to Windows 8 and later clients.

Deploying DeviceLock Service for Windows

DeviceLock Service should be installed on the computer so you can control the access to devices and network protocols on that computer. There are multiple ways to deploy DeviceLock Service to client systems.

Interactive Installation

Run Setup (**setup.exe**) and follow the instructions that appear on the screen.

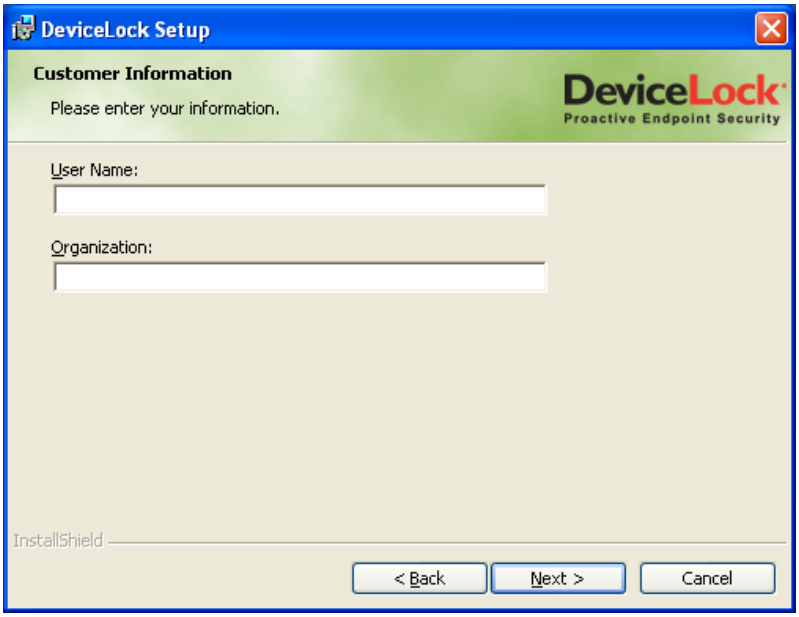

DeviceLock Setup
Welcome to the DeviceLock Setup program. This program will install DeviceLock version 7.0.0 RC1 (Build 28867) on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
InstallShield
< Back
Next >
Cancel

You should run **setup.exe** on each computer that is to be controlled with DeviceLock Service.

If you are upgrading a previous version, make sure that you have administrative access to DeviceLock Service, otherwise you will not be able to continue installation.

You must accept DeviceLock's End User License Agreement to continue the installation process.

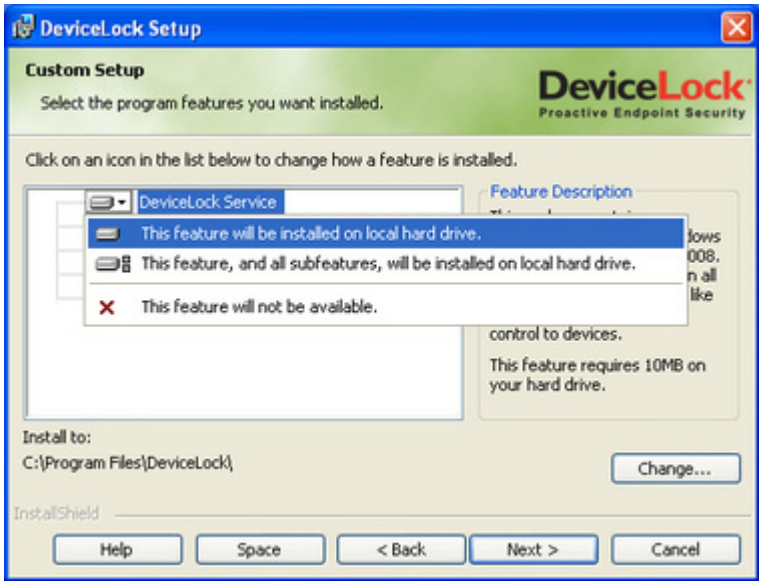
On the **Customer Information** page, type your user name and organization.



On the **Setup type** page, select the required setup type.

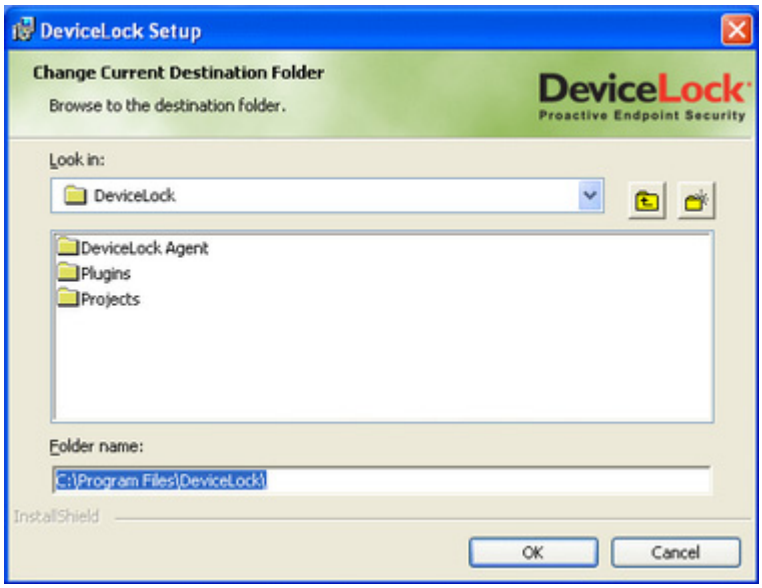
You have the following two choices: either install both DeviceLock Service and DeviceLock management consoles using the **Service + Consoles** option or install only DeviceLock Service using the **Custom** option and selecting the **DeviceLock Service** component.

DeviceLock Setup
Setup Type
Choose the setup type that best suits your needs.
DeviceLock
Proactive Endpoint Security
Please select a setup type.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
Service + Consoles
DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.
Server + Consoles
DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.
InstallShield
< Back
Next >
Cancel


DeviceLock Setup
Custom Setup
Select the program features you want installed.
DeviceLock
Proactive Endpoint Security
Click on an icon in the list below to change how a feature is installed.
DeviceLock Service
Feature Description
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
control to devices.
This feature requires 10MB on your hard drive.
Install to:
C:\Program Files\DeviceLock\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

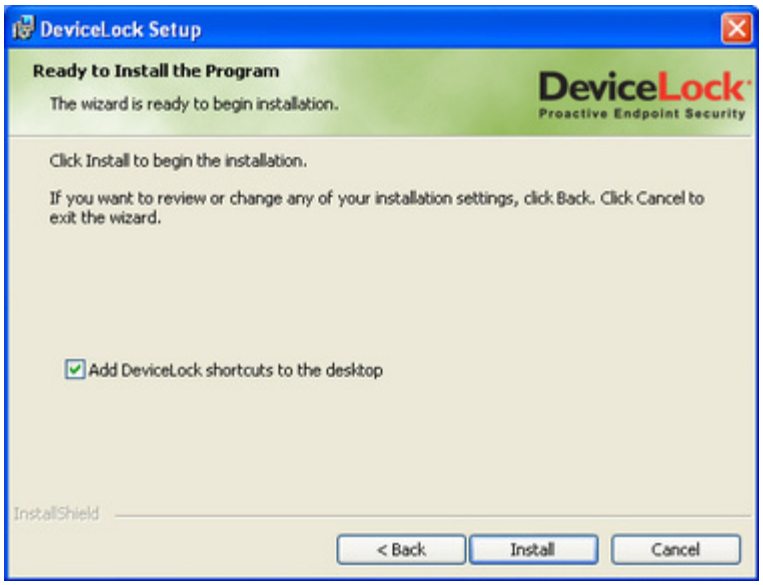
Note: On the **Custom Setup** page, you can select the RSoP component to install. This component enables support for DeviceLock's Resultant Set of Policy planning mode on domain controllers. The RSoP component is required only when DeviceLock management consoles are installed, but DeviceLock Service is not installed on the computer. For more information on RSoP planning mode, refer to the Microsoft documentation.

On the **Custom Setup** page, you can change the default installation directory. By default, the DeviceLock installation directory is **%ProgramFiles%\DeviceLock**. To change the default installation directory, click **Change** to open the **Change Current Destination Folder** page.



On the **Ready to Install the Program** page, click **Install** to begin the installation. Select the **Add DeviceLock shortcuts to the desktop** check box if you want to add

DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Service Settings Editor shortcuts to the desktop.

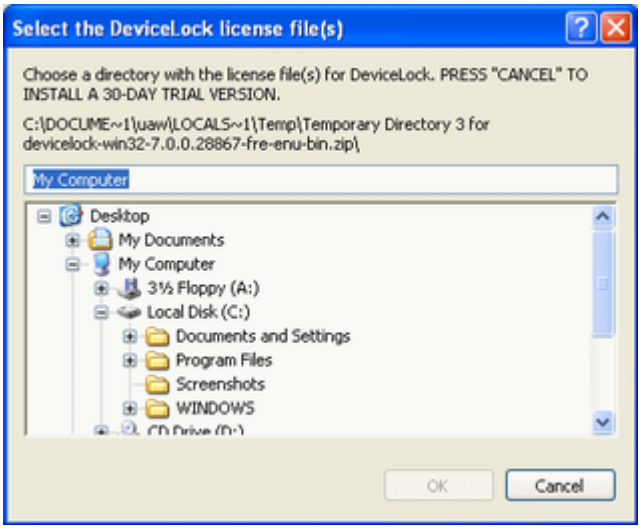

DeviceLock Setup
Ready to Install the Program
The wizard is ready to begin installation.
DeviceLock
Proactive Endpoint Security
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Add DeviceLock shortcuts to the desktop
InstallShield
< Back
Install
Cancel

If you choose to install DeviceLock management consoles as well, Setup may suggest that you generate a new DeviceLock Certificate.

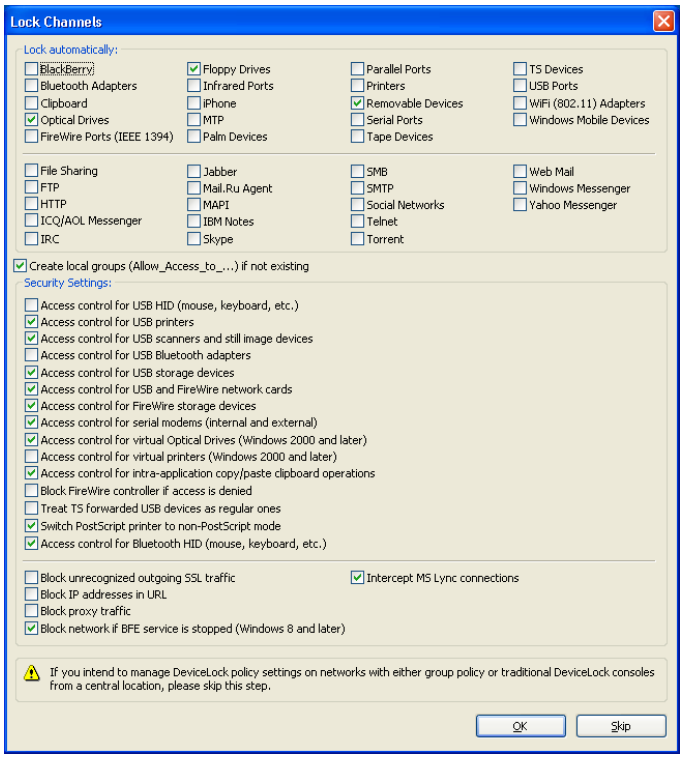
DeviceLock Setup
Do you want to create the new DeviceLock Certificate (the private and public key pair)?
Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.
Yes
No

You can always generate a new DeviceLock Certificate later, using the Certificate Generation Tool installed with DeviceLock management consoles. Hence, if at this step you are not sure whether you need the new certificate or not, just press the **No** button and continue the installation. For more information on DeviceLock Certificates, see "DeviceLock Certificates."

Also, if you select **Service + Consoles**, Setup may suggest that you load the DeviceLock license files. If you don't have the license files, click **Cancel** to install DeviceLock in a 30-day trial mode.



During the installation process, you can set special permissions for local devices and protocols.



Check devices and/or protocols you would like to set permissions to. Check the **Create local groups if not existing** flag to instruct Setup to create the special local user group Allow_Access_To_ for each channel type (e.g. Allow_Access_To_Floppy for floppy drives), if these do not exist on the local computer.

Setup assigns **Read**, **Write**, **Format** and **Eject** generic rights to members of the Administrators group and the SYSTEM account. Members of the Allow_Access_To_ group will have **Read**, **Write** and **Eject** generic rights.

Also, you can define Security Settings to exclude certain types of devices from the access check.

Check **Access control for USB HID**, **Access control for USB printers**, **Access control for USB scanners and still image devices**, **Access control for USB Bluetooth adapters**, **Access control for USB storage devices** or **Access control for FireWire storage devices** to allow DeviceLock Service to control security for Human Interface Devices (mouse, keyboard, etc.), printers, scanners and still image devices, Bluetooth adapters or storage devices (such as flash drives) plugged into the USB and FireWire port. To allow access control for USB and FireWire network cards, check **Access control for USB and FireWire network cards**. Otherwise, even if ports (USB and/or FireWire) are locked, these devices continue to function as usual. To allow access control for serial modems (internal and/or external), check **Access control for serial modems**. To disable locking of virtual (software emulated) CD/DVD/BD on Windows 2000 and later systems, uncheck **Access control for virtual Optical Drives**. To disable control of virtual printers (those which print to files) on Windows 2000 and later systems, uncheck **Access control for virtual printers**. To allow access control for copy/paste clipboard operations within an application, select the **Access control for intra-application copy/paste clipboard operations** check box. Otherwise, even if the clipboard is locked, access control for copy/paste operations within one application is disabled. To disable FireWire controllers when the Everyone account has No Access permissions for the FireWire port device type, select the **Block FireWire controller if access is denied** check box. To allow access control for Bluetooth Human Interface Devices (mouse, keyboard, etc.), check **Access control for Bluetooth HID (mouse, keyboard, etc.)**.

Select the **Switch PostScript printer to non-PostScript mode** check box to make PostScript printers act like non-PostScript printers. This resolves an issue in which DeviceLock Service is unable to create a correct shadow copy of printed data and perform content analysis of data sent to printers that use a PostScript driver.

Select the **Treat TS forwarded USB devices as regular ones** check box to allow DeviceLock Service to control access to all USB devices redirected during a Citrix XenDesktop/MS RemoteFX session according to the rights set for the USB port device type. Otherwise, DeviceLock Service controls access to all USB devices redirected during a Citrix XenDesktop/MS RemoteFX session according to the **USB Devices Access** right set for TS Devices.

Also, you can define Security Settings for protocols.

To allow DeviceLock Service to audit and block all unrecognized outgoing SSL traffic, select the **Block unrecognized outgoing SSL traffic** check box. Otherwise, even if the protocols are locked, all unrecognized outgoing SSL traffic is not blocked and audit is not performed for it.

To allow DeviceLock Service to block all URLs containing the host IP address when users have "allow access" permissions for the HTTP protocol, select the **Block IP addresses in URL** check box. Use this setting to block access to sites (for example, Facebook) that can be accessed using an IP address.

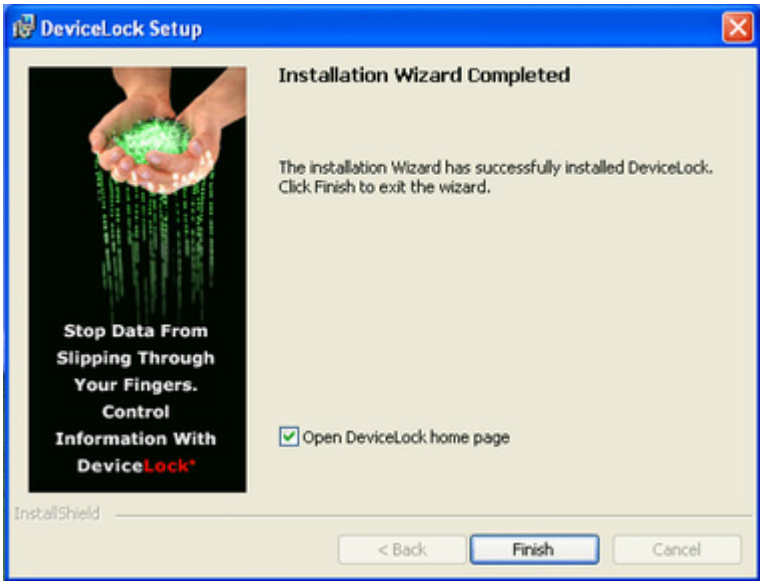
To allow DeviceLock Service to audit and block all traffic that flows through a proxy server, select the **Block proxy traffic** check box. The following proxy servers are supported: HTTP, SOCKS4, and SOCKS5.

To force DeviceLock Service to block all network traffic when the Base Filtering Engine system service is stopped, select the **Block network if BFE service is stopped (Windows 8 and later)** check box.

To allow DeviceLock Service to intercept the traffic from Microsoft Lync, Office Communicator and/or Skype for Business, select the **Intercept MS Lync connections** check box.

Click **OK** to apply changes. Click **Skip** if you prefer to wait until after installation to set permissions to these devices using DeviceLock management consoles.

As soon as Setup has installed DeviceLock, it suggests that you point your default Internet browser to the DeviceLock Web site.



Clear the **Open DeviceLock home page** check box if you do not want to visit the DeviceLock Web site. Click **Finish** to finish the installation.

Note: To uninstall DeviceLock, do one of the following:

Use **Add or Remove Programs** in Control Panel to remove **DeviceLock**.
- OR -

Click **Start**, point to **All Programs**, point to **DeviceLock**, and then click **Remove DeviceLock**.

Unattended Installation

DeviceLock also supports unattended (silent) setups. This provides an installation method that can be used from within a batch file. To install DeviceLock Service without user intervention, run Setup with the **/s** parameter (e.g. **c:\setup.exe /s**). There is a special configuration file for silent setups named ***devicelock.ini***. The devicelock.ini file must be in the same directory as setup.exe. With this file, you can customize the installation parameters.

You can open and edit devicelock.ini in any text editor, for example in Notepad. Remove a semicolon (;) before the parameter to assign a new value or leave it to assign the default value.

There are two sections (**[Install]** and **[Misc]**) in this configuration file and each section has its own parameters:

1. [Install]

To install DeviceLock Service, specify the **Service** parameter:

Service = 1

You can also install DeviceLock management consoles and the documentation, using **Manager** and **Documents** parameters.

If you want to just upgrade DeviceLock Service and do not want to change existing settings, use the **OnlyUpgradeService** parameter:

OnlyUpgradeService = 1

In this case Setup ignores all specified settings and only upgrades DeviceLock Service to the new version.

You can also define a destination directory for DeviceLock:

InstallDir = C:\Program Files\DeviceLock

Setup uses this directory if it can’t find the previous installation of DeviceLock.

If you have purchased licenses for DeviceLock, you can also specify the location of the license files:

RegFileDir = C:\Directory

where **C:\Directory** is where your license files are located.

You do not need to load the licenses, if you are installing only DeviceLock Service. They are required for DeviceLock management consoles and separately licensed components: ContentLock and NetworkLock.

To instruct DeviceLock Service to use a fixed port, specify the **FixedPort** parameter:

FixedPort = [port number]

where **port number** – the fixed TCP port number that you want to use for the communication between DeviceLock Service and management consoles. To use dynamic ports for the RPC communication, specify 0 as a port number. By default, DeviceLock Service uses port 9132.

If the **CreateGroups** parameter is set to "1", Setup creates the special local user group Allow_Access_To_ for each device type (e.g. Allow_Access_To_Floppy for floppy drives), if these do not exist on the local computer.

To apply settings, permissions, audit, shadowing rules and alerts to DeviceLock Service, specify the path to the previously saved XML file in the **SettingsFile** parameter:

SettingsFile = **C:\settings.dls**

This settings file can be created using DeviceLock Management Console, DeviceLock Group Policy Manager and/or DeviceLock Service Settings Editor.

To install DeviceLock WebConsole, specify the **WebConsole** parameter:

WebConsole = 1

During silent installation, Apache HTTP Server is installed and configured as the Web server for DeviceLock WebConsole.

To instruct the Web server to use the specified port for HTTP requests from the Web browser, specify the **Port** parameter:

Port = [port number]

The default port is 80.

To specify the Web server's host name for SSL support, use the **ServerName** parameter.

To instruct the Web server to use the specified port for HTTPS requests from the Web browser, specify the **SSLPort** parameter:

SSLPort = [port number]

The default SSL port is 443.

To specify the full path to the SSL key file, use the **SSLKeyFile** parameter.

To specify the full path to the SSL certificate file, use the **SSLCertFile** parameter.

2. [Misc]

If you want to run a program (e.g. batch file) after a successful install, you can specify the **Run** parameter:

Run = C:\mybatchfile.bat

To suppress an automatic restart even if Setup needs it, set the **DisableRestart** parameter to "1".

Installation via Microsoft Systems Management Server

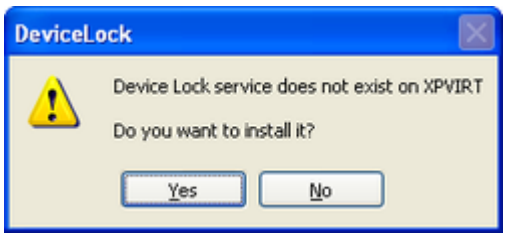
The unattended installation allows you to deploy DeviceLock Service using Microsoft Systems Management Server (SMS). Use the package definition files (DevLock.pdf for SMS version 1.x and DevLock.sms for SMS version 2.0 and later) supplied with DeviceLock, located in the sms.zip file.

Remote Installation via DeviceLock Management Console

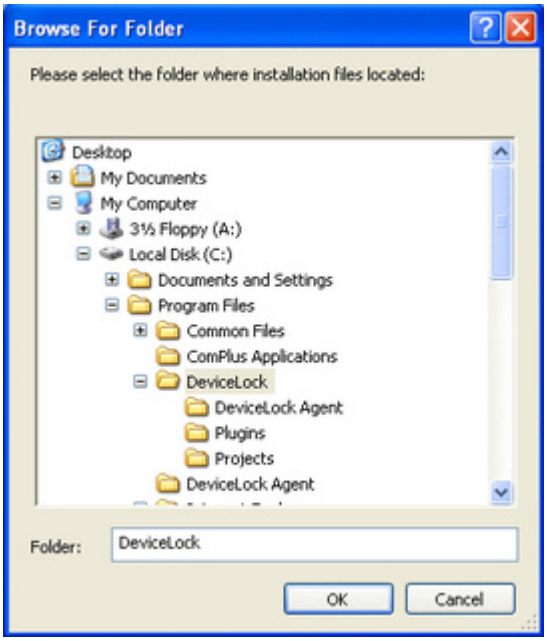
DeviceLock Management Console (the MMC snap-in) supports remote installation to help system administrators set up a service on remote machines without ever having to physically go to them.

Note: Only the built-in administrator account can be used to perform a remote installation of DeviceLock Service on computers running Windows Vista or a later version of Windows. In a Windows Active Directory environment, only members of the Domain Admins group can perform a remote installation of DeviceLock Service. Administrator privileges are required to connect to DeviceLock Service via DeviceLock Management Console. For more information, refer to Microsoft's article.

When you're trying to connect to a computer where DeviceLock Service is not installed or is outdated, the management console suggests that you install or update it.



Select the directory that contains all of the files needed for installation (such as DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe, and InstMsiW.exe).

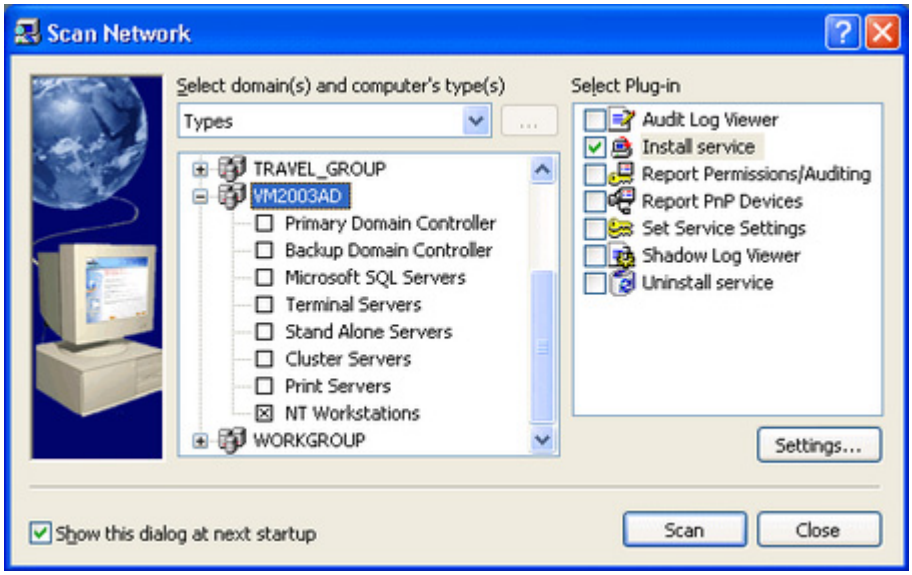


These files are located in the DeviceLock installation directory. By default, the DeviceLock installation directory is **%ProgramFiles%\DeviceLock**.

By default, the DeviceLock Service installation files will be copied to the %ProgramFiles%\DeviceLock Agent folder if this service doesn't exist on this system. If the service exists on the system but its version is lower than 7.0, the management console will also copy the installation files to the default %ProgramFiles%\DeviceLock Agent folder. If the service exists on the system but its version is 7.0 or higher, the management console will copy the installation files to the directory of the old files and the old files will be replaced.

Remote Installation via DeviceLock Enterprise Manager

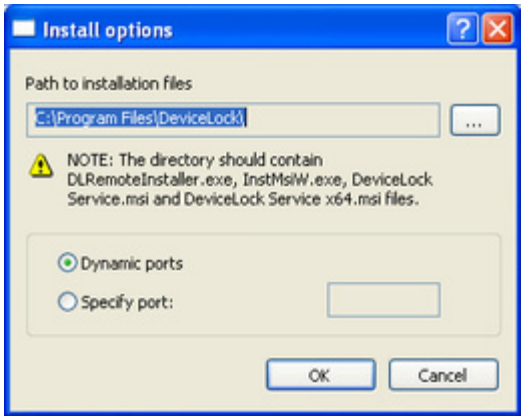
DeviceLock Enterprise Manager contains the Install service plug-in that allows you to deploy DeviceLock Service automatically on all the selected computers in your network.



Note: Only the built-in administrator account can be used to perform a remote installation of DeviceLock Service on computers running Windows Vista or a later version of Windows. In a Windows Active Directory environment, only members of the Domain Admins group can perform a remote installation of DeviceLock Service. Administrator privileges are required to connect to DeviceLock Service via DeviceLock Management Console. For more information, refer to Microsoft's article.

First, select computers where DeviceLock Service must be installed. DeviceLock Enterprise Manager allows you to select computers by their types and names. You can also load the computers list from an external file or select them from any LDAP tree (Active Directory, Novell eDirectory, OpenLDAP and so on).

Then, select the **Install service** plug-in and click the **Settings** button to specify the directory that contains all of the files needed for installation (such as DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe, and InstMsiW.exe). These files are located in the DeviceLock installation directory. By default, the DeviceLock installation directory is **%ProgramFiles%\DeviceLock**. You can also instruct DeviceLock Service to use the fixed TCP port for the communication with management consoles. To use dynamic ports for the RPC communication, select the **Dynamic ports** option. By default, DeviceLock Service uses port 9132.



By default, the DeviceLock Service installation files will be copied to the %ProgramFiles%\DeviceLock Agent folder if this service doesn't exist on this system. If the service exists on the system but its version is lower than 7.0, the Install service plug-in will also copy the installation files to the default %ProgramFiles%\DeviceLock Agent folder. If the service exists on the system but its version is 7.0 or higher, the Install service plug-in will copy the installation files to the directory of the old files and the old files will be replaced.

Installation via Group Policy

This step-by-step instruction describes how to use Group Policy to automatically distribute DeviceLock Service to client computers. DeviceLock Service can be deployed in an Active Directory domain using the Microsoft Software Installer (MSI) package (DeviceLock Service.msi and DeviceLock Service x64.msi).

Note: Microsoft Windows Group Policy automated-program installation requires client computers that are running Windows 2000 or later.

If you use a custom MSI package with defined DeviceLock Service settings to deploy DeviceLock Service using Group Policy, these settings are not applied to client computers if any one of the following conditions is true:

- The default security is disabled on remotely running DeviceLock Services.

- The GPO applied to client computers has the **Override Local Policy** setting enabled.

For information about how to create a custom MSI package, see "Create MSI Package."

You can use Group Policy to distribute DeviceLock Service by using the following steps:

- **Create a Distribution Point**

  To install DeviceLock Service, you must create a distribution point on the server. To create a distribution point, do the following:

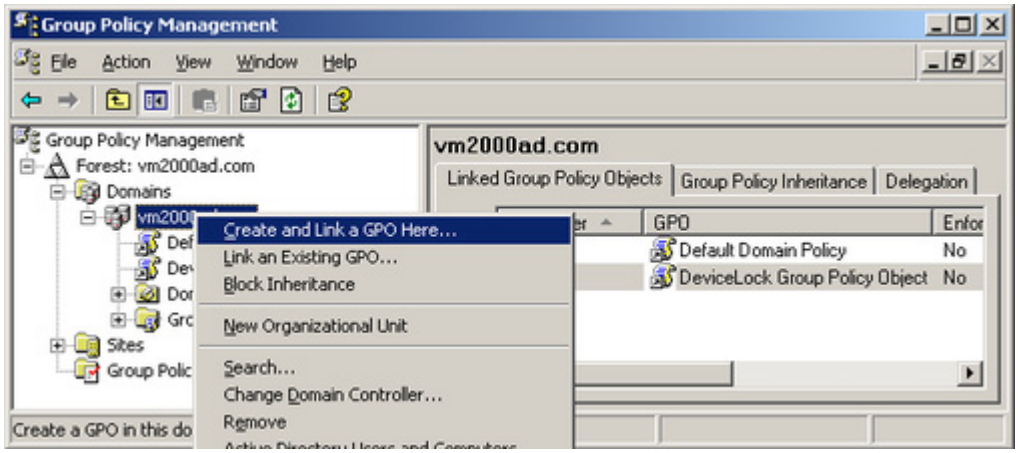
  1. Log on to the server computer as an administrator.
  2. Create a shared network folder in which to place the MSI package.
  3. Set permissions on the share to allow access to the distribution package.
  4. Copy the MSI package (DeviceLock Service.msi and/or DeviceLock Service x64.msi) to the distribution point.

- **Create a Group Policy Object**

  To create a Group Policy object (GPO) with which to distribute DeviceLock Service, do the following:

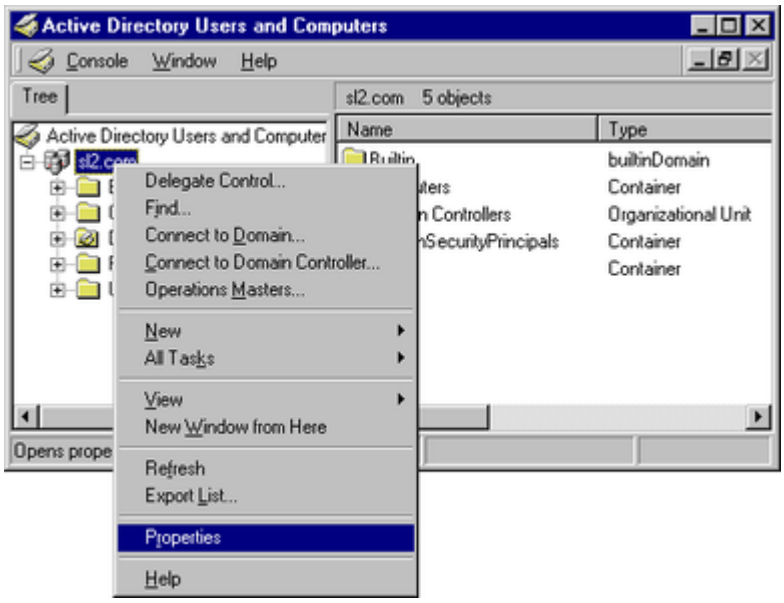
  1. Start the Group Policy Management snap-in.
     If the Group Policy Management snap-in is not installed on your computer, you may use the Active Directory Users and Computers snap-in instead.

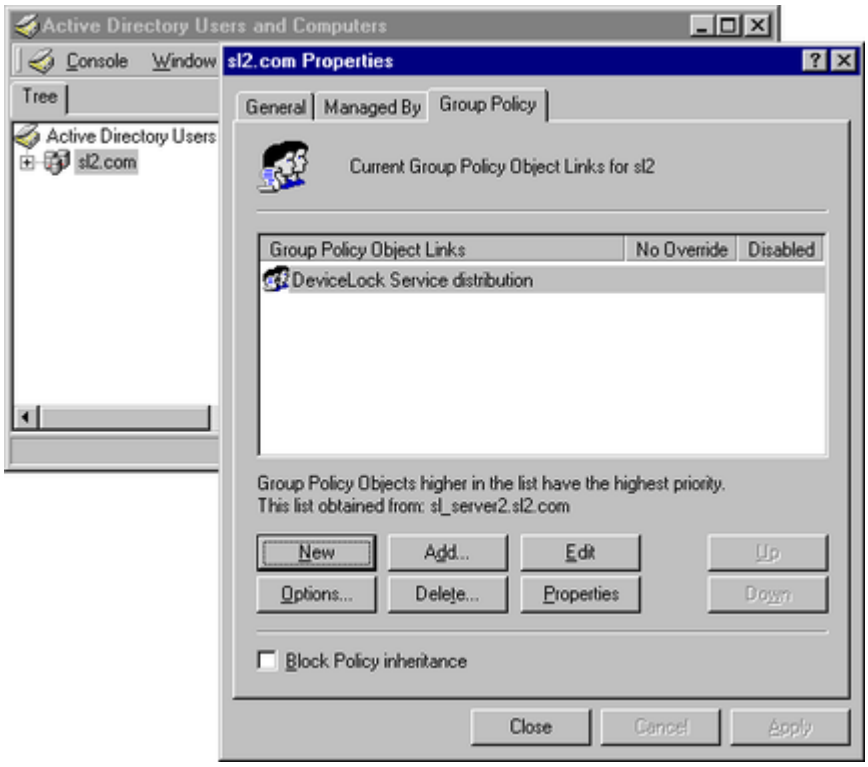
2. In the console tree, select your domain.



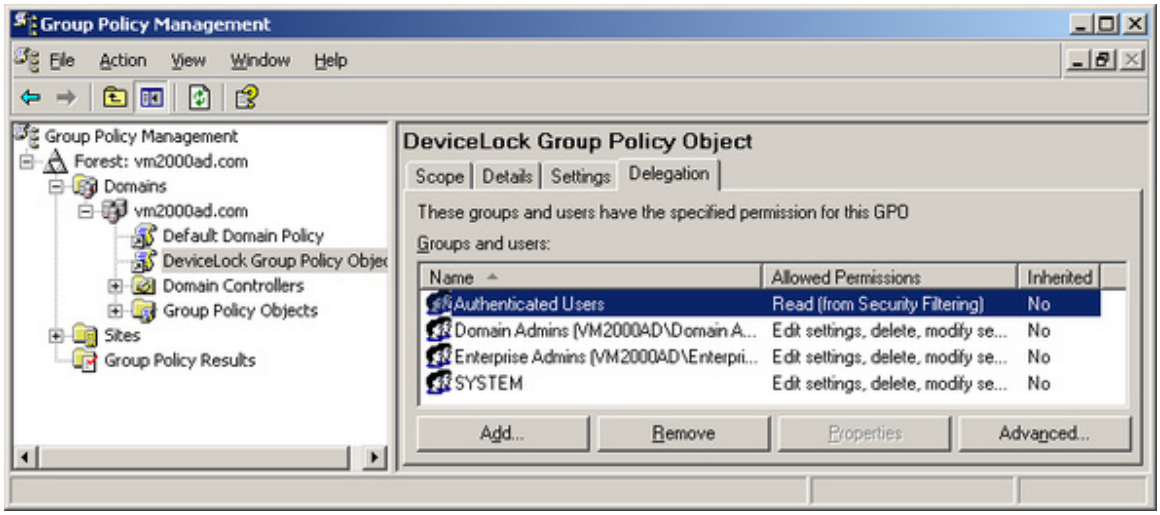
3. Click **Create and Link a GPO Here** from the context menu of the domain item.

   If you are using the Active Directory Users and Computers snap-in, right-click your domain, then click **Properties**, click the Group Policy tab, and then click **New**.

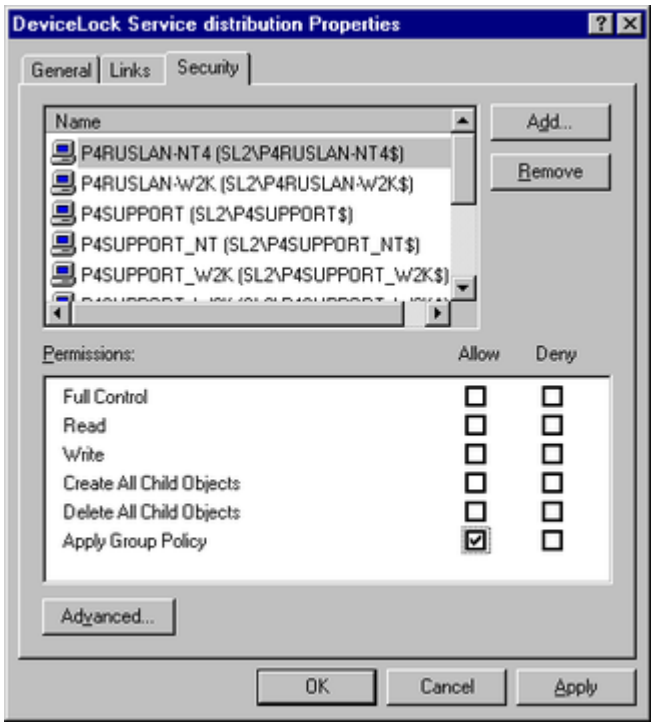




4. Type the name that you want to call this policy, and then press ENTER.
5. In the console tree, select your group policy object, click the **Delegation** tab, and then click **Advanced**.



If you are using the Active Directory Users and Computers snap-in, click **Properties** on the **Group Policy** tab, and then click the **Security** tab.



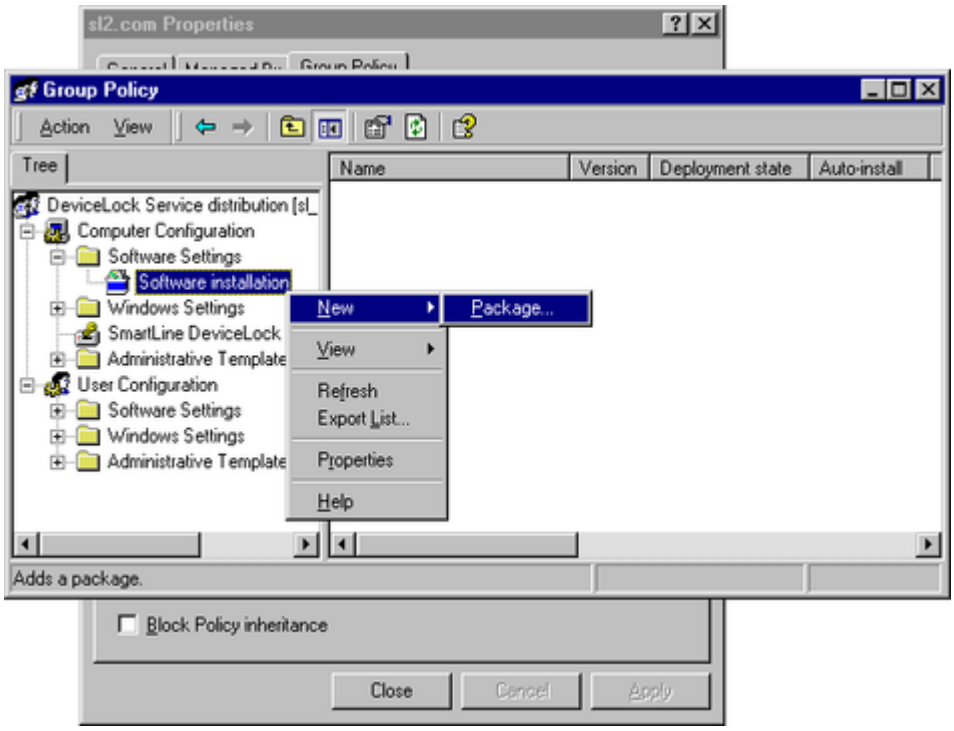
6. Click on the **Deny** check box next to **Apply Group Policy** for the security groups that you want to prevent from having this policy applied.

   Click on the **Allow** check box for the groups to which you want to apply this policy. When you are finished, click **OK**.

- **Assign a Package**

  To assign DeviceLock Service to computers that are running Windows 2000 or later:

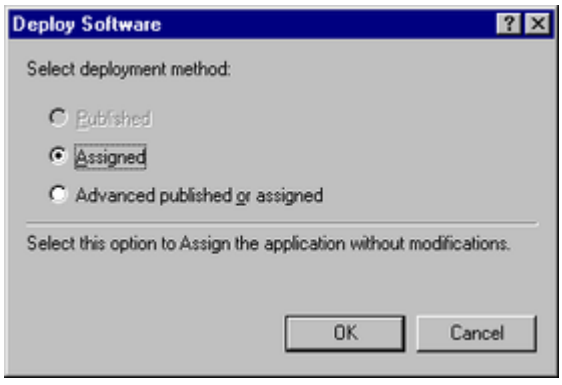
  1. Open the group policy object that you need in the Windows Group Policy Object editor (use either the Group Policy Management or Active Directory Users and Computers snap-in).
  2. Under **Computer Configuration**, expand **Software Settings**.
  3. Right-click **Software installation**, point to **New**, and then click **Package**.



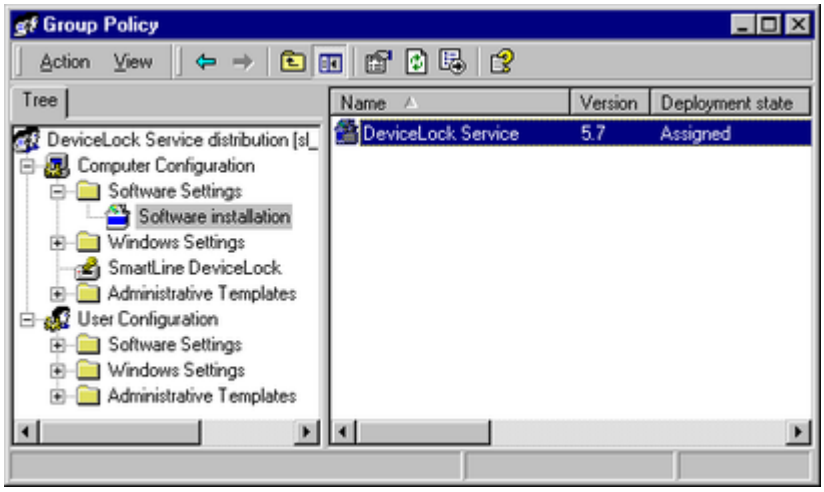
4. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path to the shared folder that contains the DeviceLock Service MSI package. For example: \\file server\share\DeviceLock Service.msi.

Important: Do not browse to the location. Ensure that you use the UNC path to the shared folder.

5. Click **Open**.
6. Click **Assigned**, and then click **OK**.
   The package is listed in the right pane of the Group Policy window.



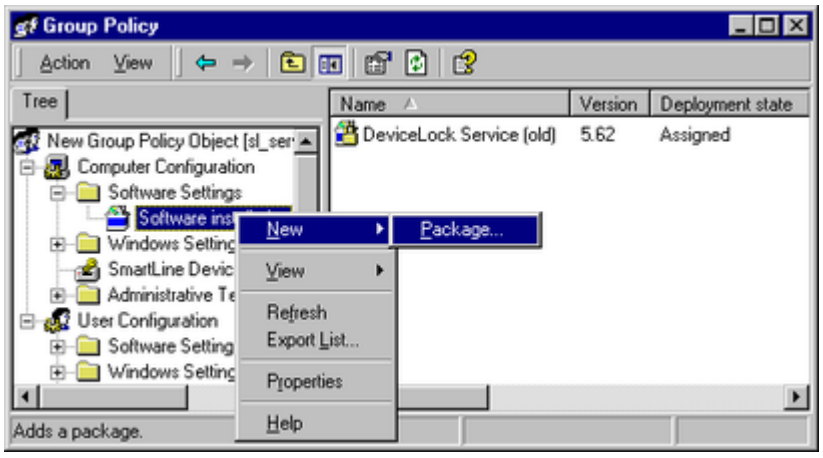
7. Close the Windows Group Policy Object editor. When the client computer starts, DeviceLock Service is automatically installed.



- **Upgrade a Package**

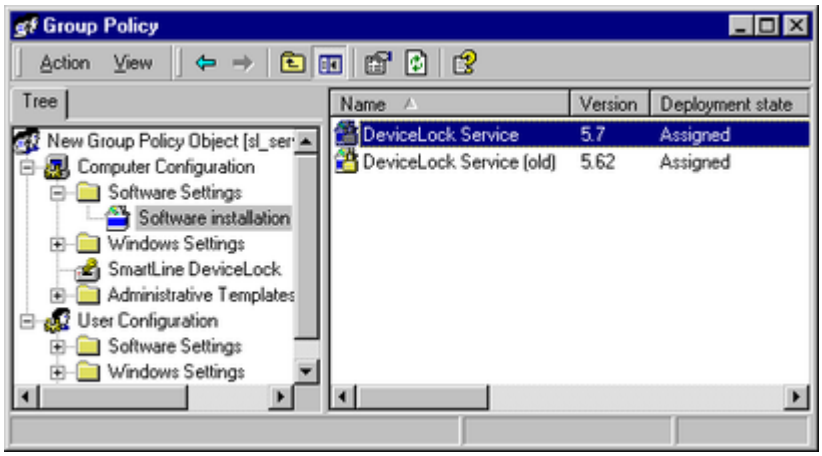
  If the previous version of DeviceLock Service was already deployed and you want to upgrade it to the new one:

  1. Open the group policy object that contains the old DeviceLock Service package in the Windows Group Policy Object editor (use either the Group Policy Management or Active Directory Users and Computers snap-in).
  2. Under **Computer Configuration**, expand **Software Settings**.
  3. Right-click **Software installation**, point to **New**, and then click **Package**.

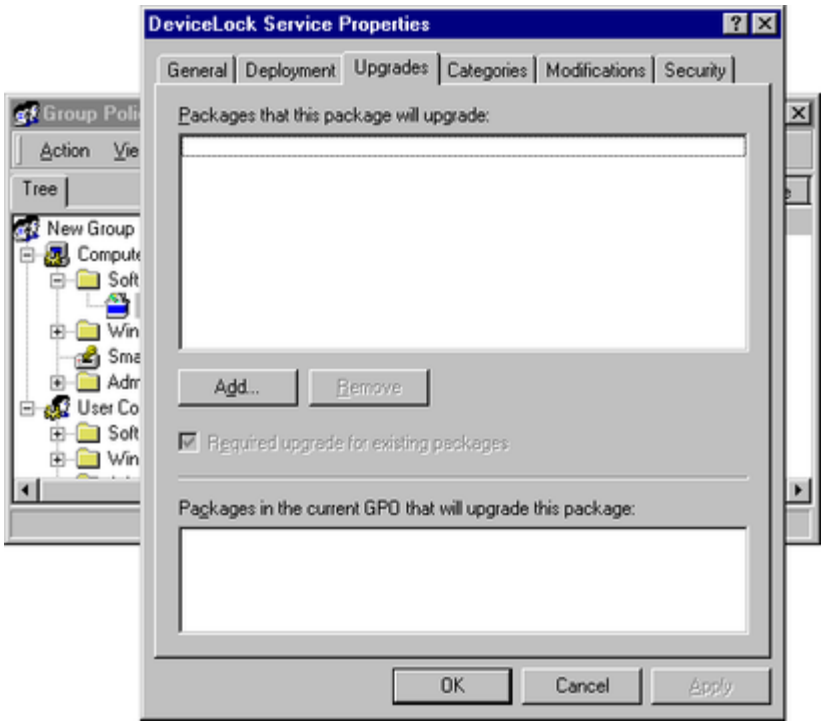


  4. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path to the shared folder that contains the new DeviceLock Service MSI package. For example: \\file server\share\DeviceLock Service.msi.
  5. Click **Open**.
  6. Click **Assigned**, and then click **OK**.

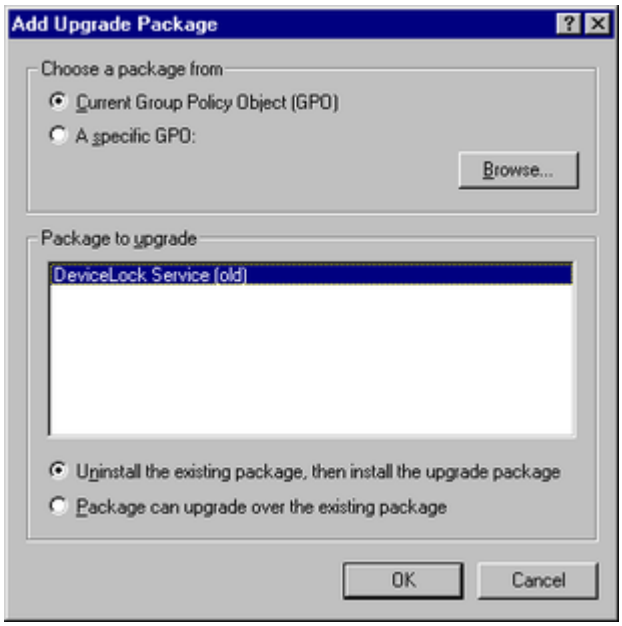
The new package is listed in the right pane of the Group Policy window.



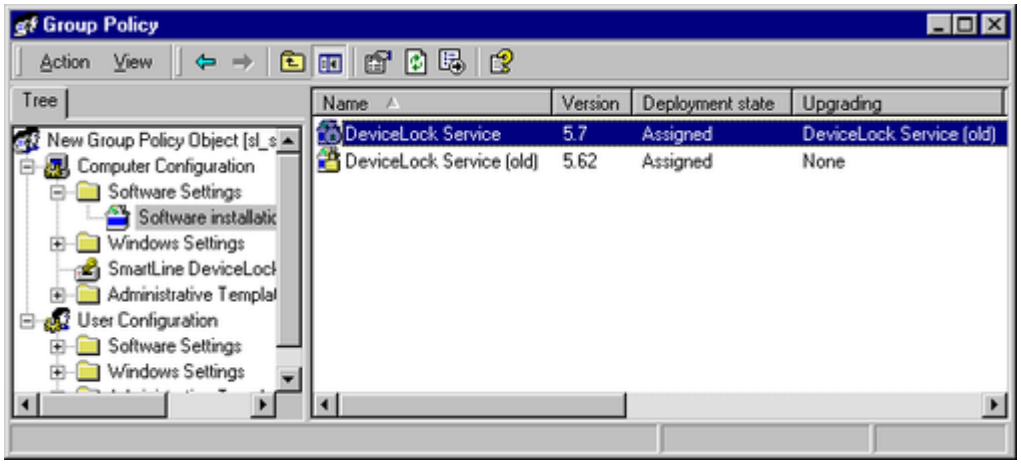
7. Right-click the new package, click **Properties**, and then click the **Upgrades** tab.



8. Click **Add**, select the old DeviceLock Service package you want to upgrade, click **Uninstall the existing package, then install the upgrade package**, and then click **OK**.



9. Click **OK** to close the **Properties** window, close the Windows Group Policy Object editor. When the client computer starts, DeviceLock Service is automatically upgraded.



Note: Usually when you upgrade, the new DeviceLock Service MSI package detects its previously assigned package in GPO and automatically performs steps 7 and 8 described above.

- **Redeploy a Package**

  In some cases you may want to redeploy DeviceLock Service.

  To redeploy a package:

  1. Open the group policy object which contains the deployed package in the Windows Group Policy Object editor (use either the Group Policy Management or Active Directory Users and Computers snap-in).
  2. Expand the **Software Settings** container that contains the **Software installation** item with which you deployed the package.

3. Click the **Software installation** container that contains the package.
4. In the right pane of the **Group Policy** window, right-click the program, point to **All Tasks**, and then click **Redeploy application**.
   The following message is displayed: "Redeploying this application will reinstall the application everywhere it is already installed. Do you want to continue?"
5. Click **Yes**.
6. Close the Windows Group Policy Object editor.

- **Remove a Package**

  To remove DeviceLock Service:

  1. Open the group policy object which contains the deployed package in the Windows Group Policy Object editor (use either the Group Policy Management or Active Directory Users and Computers snap-in).
  2. Expand the **Software Settings** container that contains the **Software installation** item with which you deployed the package.
  3. Click the **Software installation** container that contains the package.
  4. In the right pane of the **Group Policy** window, right-click the program, point to **All Tasks**, and then click **Remove**.
  5. Click **Immediately uninstall the software from users and computers**, and then click **OK**.
  6. Close the Windows Group Policy Object editor.

Please keep in mind:

- Deployment occurs only when the computer starts up, not on a periodic basis. This prevents undesirable results, such as uninstalling or upgrading an application that is in use.
- DeviceLock Service will be copied to the %ProgramFiles%\DeviceLock Agent folder if this service doesn't exist on the system. If the service exists on the system but its version is lower than 7.0, DeviceLock Service will also be copied to the default %ProgramFiles%\DeviceLock Agent folder. If the service exists on the system but its version is 7.0 or higher, DeviceLock Service will be copied to the directory of the old version and the old version will be replaced.

Installation via DeviceLock Enterprise Server

This step-by-step instruction describes how to use DeviceLock Enterprise Server component to automatically distribute DeviceLock Service to client computers. DeviceLock Service can be deployed using the Microsoft Software Installer (MSI) package (DeviceLock Service.msi and DeviceLock Service x64.msi).

Note: If you use a custom MSI package with defined DeviceLock Service settings to deploy DeviceLock Service using DeviceLock Enterprise Server, these settings are not applied to client computers if any one of the following conditions is true:

- The name of the MSI package is different from **DeviceLock Service.msi** or **DeviceLock Service x64.msi;**
- The first 3 digits of DeviceLock Service version number do not match those of DeviceLock Enterprise Server.

For information about how to create a custom MSI package, see "Create MSI Package."

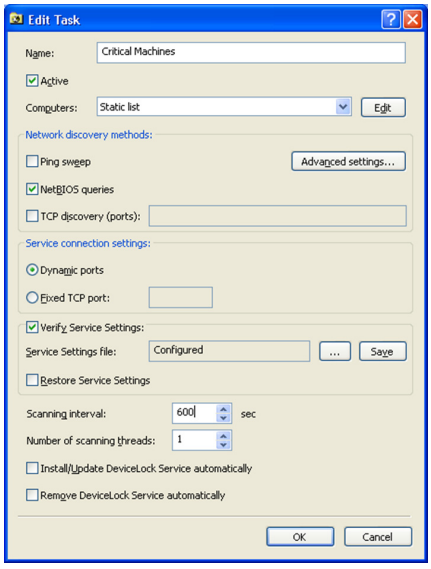
You can use DeviceLock Enterprise Server to distribute DeviceLock Service by creating a Monitoring task.

To install DeviceLock Service, you must create a Monitoring task on DeviceLock Enterprise Server. To create a task, do the following:

- Launch **DeviceLock Management Console**, or **DeviceLock Webconsole**
- Connect to **DeviceLock Enterprise Server**
- Create a Monitoring task

Note: For information about how to create a Monitoring task, see "Create / Modify task."

- To install DeviceLock Service to a selected list of computers, check the **Install/update DeviceLock Service automatically** flag
- Make sure the **Active** flag in the upper left corner of task dialog is checked, then click **OK**. DeviceLock Enterprise Server installs DeviceLock Service to a selected list of computers when the task is executed.



Note: To automatically remove DeviceLock Service from selected list of computers, check **Remove DeviceLock Service automatically** flag when editing a Monitoring task.

Deploying DeviceLock Service for Mac

DeviceLock Service for Mac should be installed on the computer so you can control the access to devices on that computer. There are multiple ways to deploy DeviceLock Service for Mac to client systems.

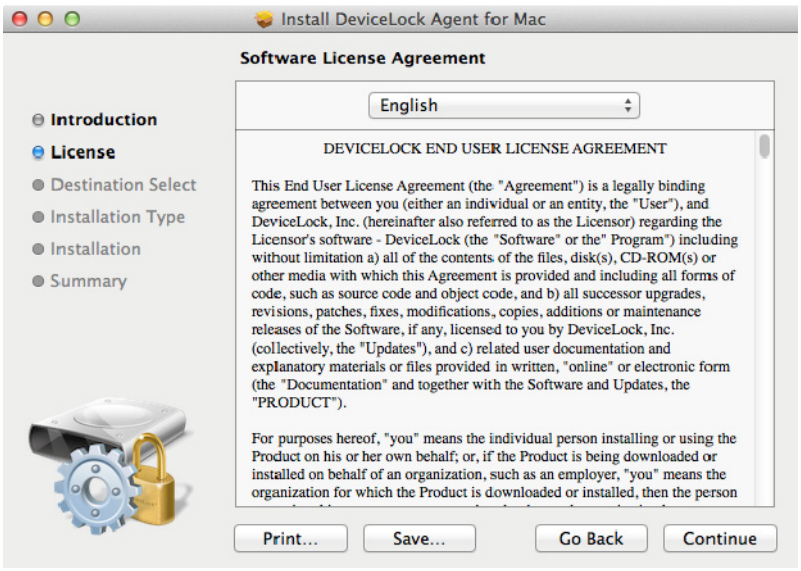
First of all, mount **DeviceLock Service.dmg**.

Interactive Installation

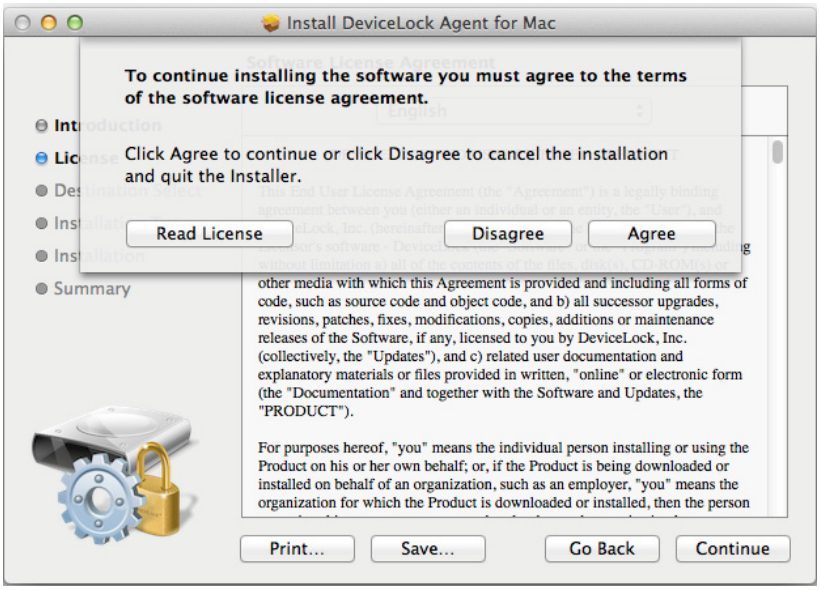
Interactive installation is engaged by launching the installation package. To install DeviceLock Service for Mac in interactive mode, launch **DeviceLock Service.pkg** and follow the instructions that appear on the screen.

You should run **DeviceLock Service.pkg** on each computer that is to be controlled with DeviceLock Service for Mac.

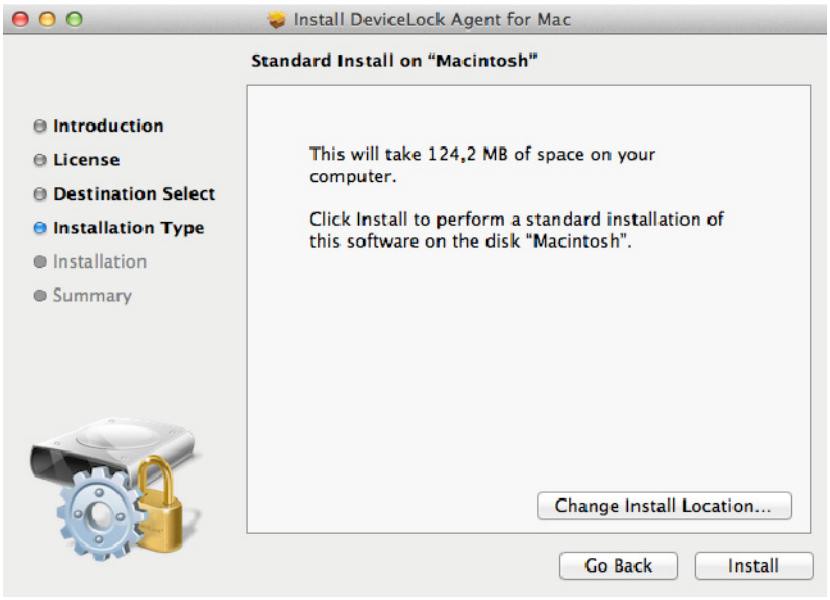
If you are upgrading a previous version, make sure that you have administrative access to DeviceLock Service for Mac; otherwise you will not be able to continue installation.


Install DeviceLock Agent for Mac
Software License Agreement
Introduction
License
Destination Select
Installation Type
Installation
Summary
English
DEVICELOCK END USER LICENSE AGREEMENT
This End User License Agreement (the "Agreement") is a legally binding agreement between you (either an individual or an entity, the "User"), and DeviceLock, Inc. (hereinafter also referred to as the Licensor) regarding the Licensor's software - DeviceLock (the "Software" or the" Program") including without limitation a) all of the contents of the files, disk(s), CD-ROM(s) or other media with which this Agreement is provided and including all forms of code, such as source code and object code, and b) all successor upgrades, revisions, patches, fixes, modifications, copies, additions or maintenance releases of the Software, if any, licensed to you by DeviceLock, Inc. (collectively, the "Updates"), and c) related user documentation and explanatory materials or files provided in written, "online" or electronic form (the "Documentation" and together with the Software and Updates, the "PRODUCT").
For purposes hereof, "you" means the individual person installing or using the Product on his or her own behalf; or, if the Product is being downloaded or installed on behalf of an organization, such as an employer, "you" means the organization for which the Product is downloaded or installed, then the person
Print...
Save...
Go Back
Continue

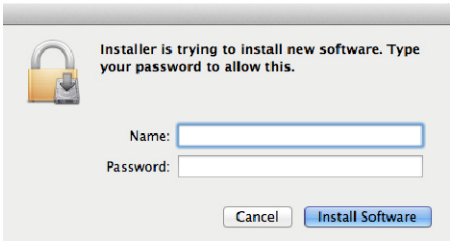
You will be presented with DeviceLock End User License Agreement. You may print or save the text of this License Agreement for future reference. Click **Continue** to proceed to the next step.


Install DeviceLock Agent for Mac
To continue installing the software you must agree to the terms of the software license agreement.
Click Agree to continue or click Disagree to cancel the installation and quit the Installer.
Read License
Disagree
Agree
Summary
other media with which this Agreement is provided and including all forms of code, such as source code and object code, and b) all successor upgrades, revisions, patches, fixes, modifications, copies, additions or maintenance releases of the Software, if any, licensed to you by DeviceLock, Inc. (collectively, the "Updates"), and c) related user documentation and explanatory materials or files provided in written, "online" or electronic form (the "Documentation" and together with the Software and Updates, the "PRODUCT").
For purposes hereof, "you" means the individual person installing or using the Product on his or her own behalf; or, if the Product is being downloaded or installed on behalf of an organization, such as an employer, "you" means the organization for which the Product is downloaded or installed, then the person
Print...
Save...
Go Back
Continue

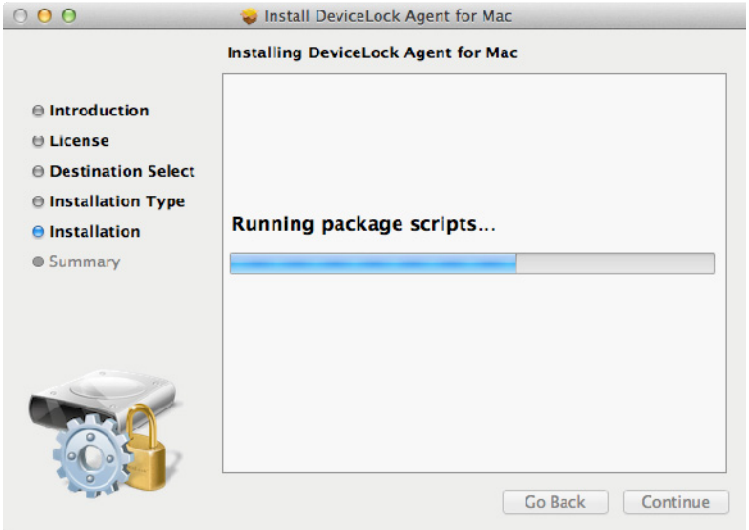
You will need to read and accept DeviceLock End User License Agreement before continuing installation. Click **Continue** to proceed to the next step.



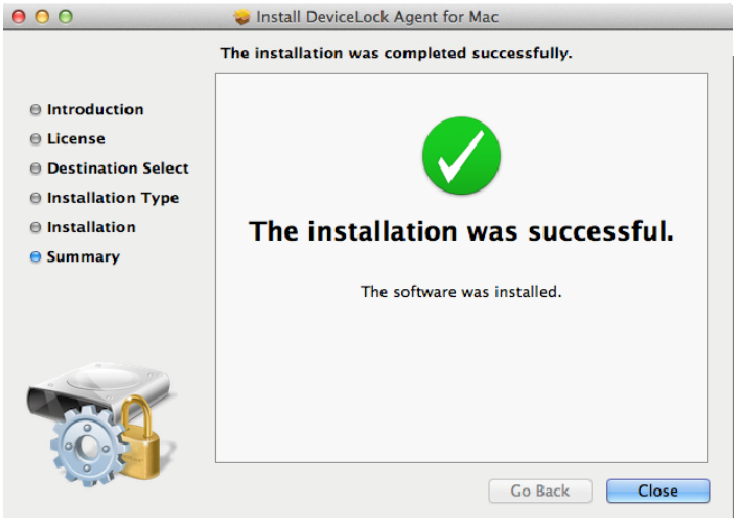
You will be informed on the amount of disk space required for installing DeviceLock Service for Mac. At this point, DeviceLock Service for Mac is ready to be installed. Click **Install** to continue.



You will need to authenticate with administrative credentials in order to be able to install DeviceLock Service for Mac. Enter user name and password of a user having administrative privileges, and click **Install Software** to continue.



A dialog window with a progress bar will be displayed. The installation may take several minutes. You cannot interrupt DeviceLock Service for Mac installation. Should you need to uninstall the product later on, please follow the standard software uninstallation procedure.



After a few minutes, the installation is complete. Click **Close** to close the installer.

Command Line Utility

Installation is also possible by using a command-line utility. This utility can install DeviceLock Service for Mac in interactive or unattended mode. Do note, however, that you will need to have administrative access to the computer you will be installing DeviceLock Service for Mac on.

The command line utility is located at /Library/DeviceLockAgent/Utilities/install. The utility can be placed (copied) to any other directory. A single .pkg file should be placed along with this utility in the same directory. It is essential to only place a single .pkg file; otherwise, if running the installation tool without parameters, a random package may be installed.

The command line tool can work in either interactive or unattended (silent) mode. Use the command line utility to install DeviceLock Service for Mac as follows.

While there are several ways to install DeviceLock Service for Mac, making use of the following command is recommended:

sudo install --delayed --package *path_to_package* **--settings** *path_to_ini_file*

The **--settings** parameter is optional.

Note: If the computer you are installing DeviceLock Service for Mac to runs Python 3 or older, use the following command:

sudo python2.7 install --delayed --package *path_to_package* **--settings** *path_to_ini_file*
or
sudo python2.6 install --delayed --package *path_to_package* **--settings** *path_to_ini_file*

By default, Apple distributes its systems with Python 2.6 or 2.7.

For example:

sudo /Volumes/DeviceLock/Utilities/install --delayed --package /Volumes/DeviceLock/DeviceLockAgent.pkg --settings /Users/admin/devicelock.ini

If DeviceLock Service for Mac is being installed for the first time, the above command will launch silent (unattended) installation. Otherwise, the system will update or reinstall DeviceLock Service for Mac upon computer reboot.

When reinstalling or upgrading DeviceLock Service for Mac, interactive installation is not recommended as the updated service will start working only after reboot.

Unattended Installation

To install DeviceLock Service for Mac without user intervention, you will need using the command line installation tool in the silent mode.

Unattended installation is launched when running the installation tool with **--silent** or **--delayed** parameters in the command line. The use of **--delayed** parameter implicitly means **--silent**. Note that, depending on whether or not the "root" user appears in the list of DeviceLock Administrators, the installation tool will exhibit different behavior:

- If the installation utility is launched without specifying a .pkg file, it will install the first .pkg file located in the same directory where the tool is located. If there are several .pkg files in that directory, a random one may be installed.
- A specific .pkg file can be used by appending the full file name after the **--package** key. The keys can be used in any order. Relative file names are supported.
- Finally, the installation utility will perform a silent install if "root" is not included in the list of DeviceLock Administrators. If this is the case, the installation tool will copy the .pkg file into the /Library/DeviceLockPackages directory. The service will reinstall or update on next reboot.

You can configure DeviceLock Service for Mac automatically immediately after the installation. In order to pre-configure DeviceLock Service for Mac during the

installation, edit **devicelock.ini** by adding the path to the .dls settings file. You can use a local or network path.

Note: The format of devicelock.ini is identical to its Windows counterpart. However, only a single parameter is supported. At this time, you can only use the SettingsFile parameter to specify the path to the previously saved XML file that must be used to configure DeviceLock Service for Mac immediately after the installation.

For example:

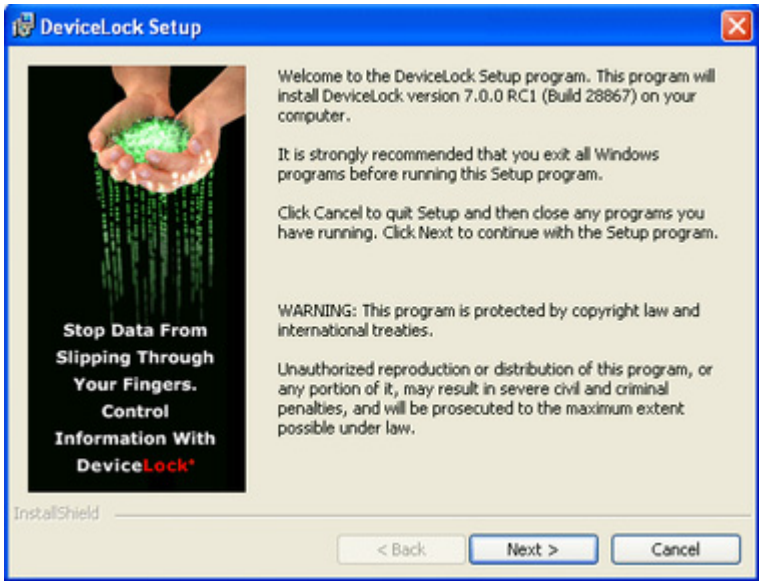
sudo /MyDirectory/install --silent --package /SomeDir/DeviceLock.pkg --settings /SomeDir/devicelock.ini

Installing Management Consoles

DeviceLock management consoles are the control interfaces that systems administrators use to remotely manage DeviceLock Service, DeviceLock Enterprise Server and DeviceLock Content Security Server.

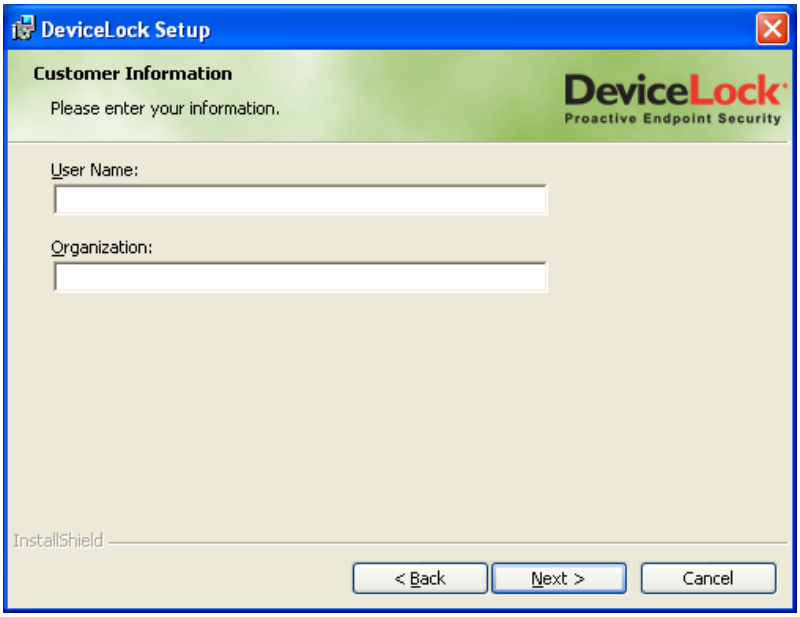
The DeviceLock management consoles should be installed on the computer from which the administrator is going to manage DeviceLock's settings and run reports. It is not necessary to install management consoles on the server (domain controller or others), even if you are going to use DeviceLock Group Policy Manager to manage settings via Active Directory Group Policy – you can do it from your local workstation (proper privileges required).

Run Setup (**setup.exe**) and follow the instructions that appear on the screen.


DeviceLock Setup
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
Welcome to the DeviceLock Setup program. This program will install DeviceLock version 7.0.0 RC1 (Build 28867) on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
InstallShield
< Back
Next >
Cancel

You must accept the DeviceLock's End User License Agreement before continuing the installation process.

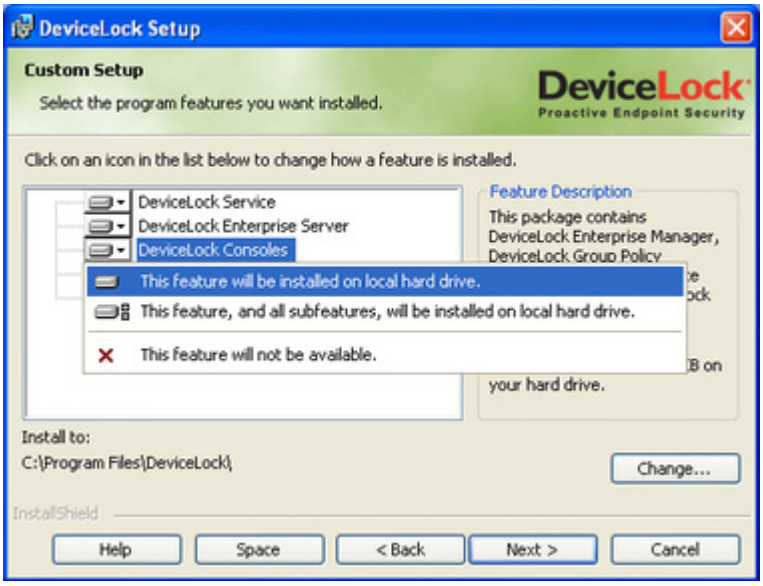
On the **Customer Information** page, type your user name and organization.



On the **Setup type** page, select the required setup type.

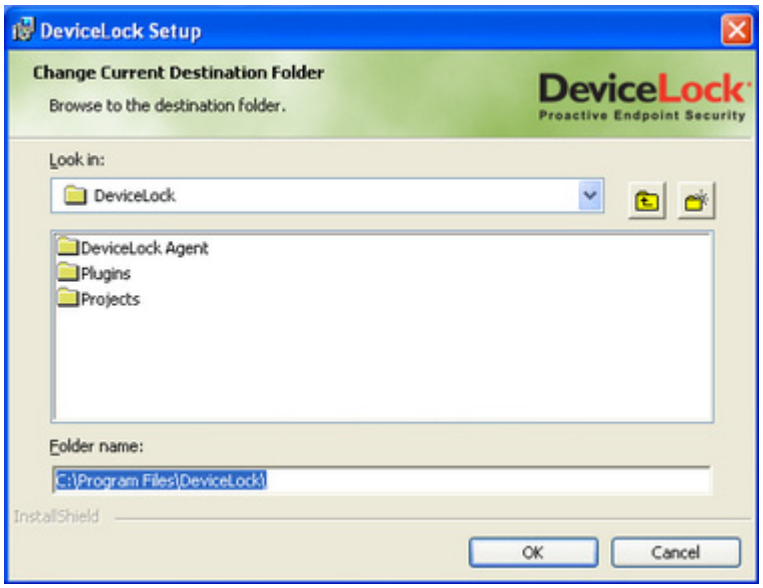
You have the following three choices: install both DeviceLock Service and DeviceLock management consoles using the **Service + Consoles** option, install both DeviceLock Enterprise Server and DeviceLock management consoles using the **Server + Consoles** option or install only DeviceLock management consoles using the **Custom** option and selecting the **DeviceLock Consoles** component.

DeviceLock Setup
Setup Type
Choose the setup type that best suits your needs.
DeviceLock
Proactive Endpoint Security
Please select a setup type.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
Service + Consoles
DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.
Server + Consoles
DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.
InstallShield
< Back
Next >
Cancel



Note: On the **Custom Setup** page, you can select the RSoP component to install. This component enables support for DeviceLock's Resultant Set of Policy planning mode on domain controllers. The RSoP component is required only when DeviceLock management consoles are installed, but DeviceLock Service is not installed on the computer. For more information on RSoP planning mode, refer to the Microsoft documentation.

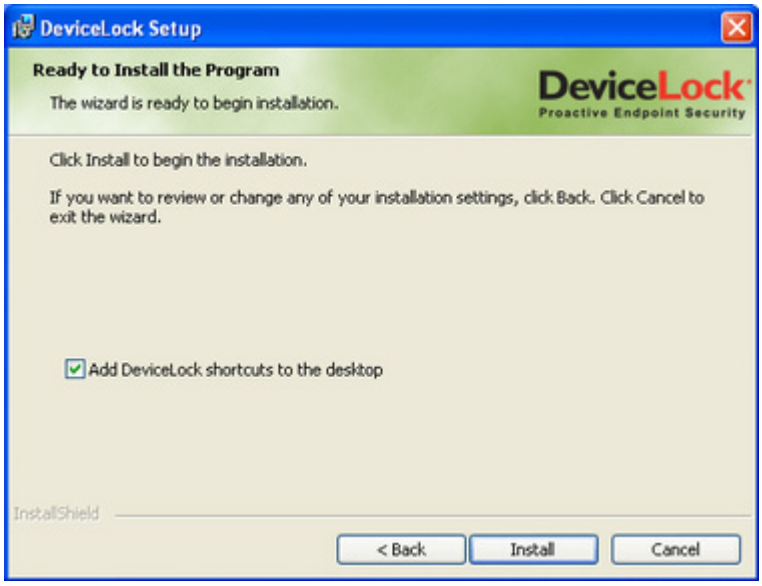
On the **Custom Setup** page, you can change the default installation directory. By default, the DeviceLock installation directory is **%ProgramFiles%\DeviceLock**. To change the default installation directory, click **Change** to open the **Change Current Destination Folder** page.



DeviceLock ships with four different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager, DeviceLock WebConsole and DeviceLock Group Policy Manager (integrates into the Windows Group Policy

Editor). Installed together with other management consoles is DeviceLock Service Settings Editor, a tool used for creating and modifying external XML files with settings, permissions, audit, shadowing rules and alerts for DeviceLock Service.

On the **Ready to Install the Program** page, click **Install** to begin the installation. Select the **Add DeviceLock shortcuts to the desktop** check box if you want to add DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Service Settings Editor shortcuts to the desktop.

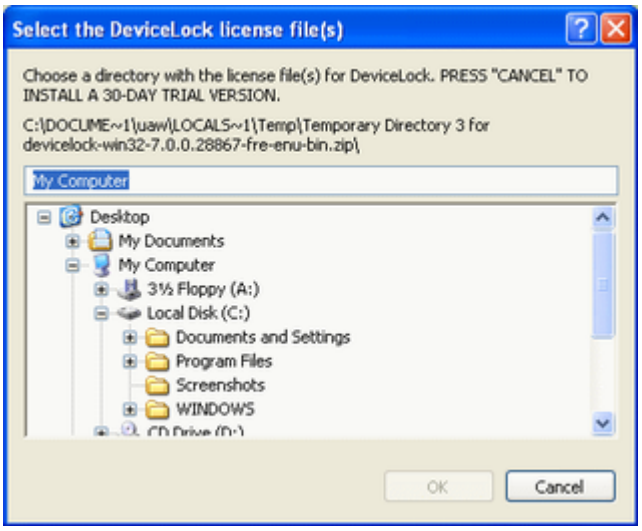

DeviceLock Setup
Ready to Install the Program
The wizard is ready to begin installation.
DeviceLock
Proactive Endpoint Security
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Add DeviceLock shortcuts to the desktop
InstallShield
< Back
Install
Cancel

Setup may suggest that you generate a new DeviceLock Certificate.

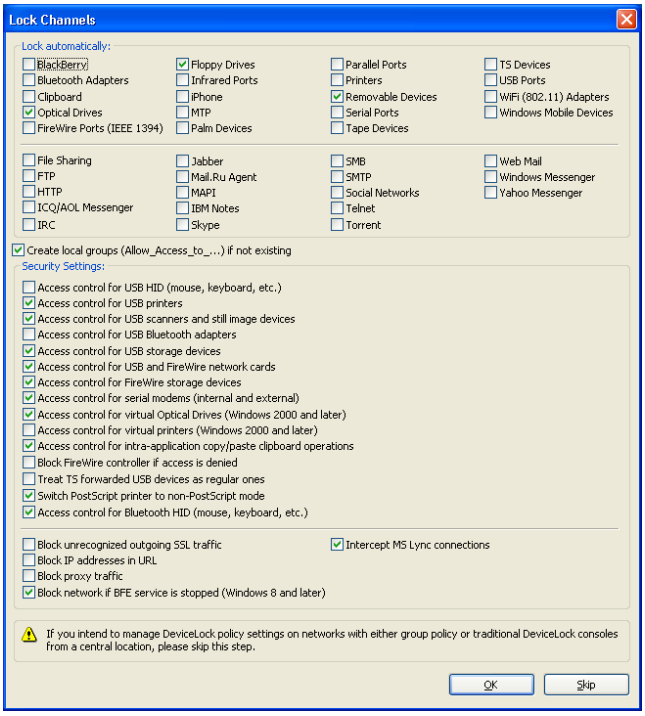
DeviceLock Setup
Do you want to create the new DeviceLock Certificate (the private and public key pair)?
Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.
Yes
No

You can always generate the new DeviceLock Certificate later, using the Certificate Generation Tool installed with DeviceLock management consoles. Hence, if at this step you are not sure whether you need the new certificate or not, just press the **No** button and continue the installation. For more information on DeviceLock Certificates, see "DeviceLock Certificates."

Also, Setup may suggest that you load the license files for DeviceLock. If you don't have the license files, click **Cancel** to install DeviceLock in a 30-day trial mode.

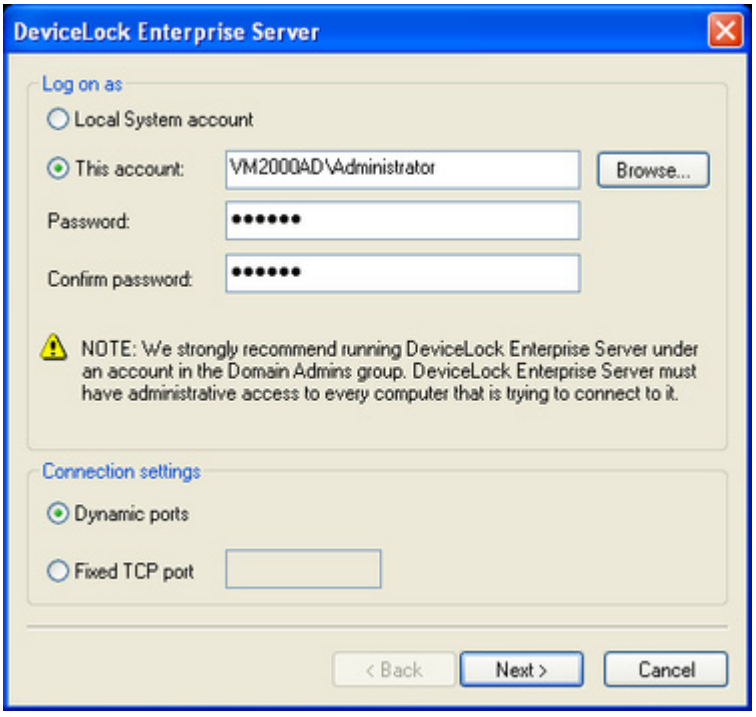


If you opted to install DeviceLock Service as well, Setup suggests that you set special permissions for local devices and protocols.



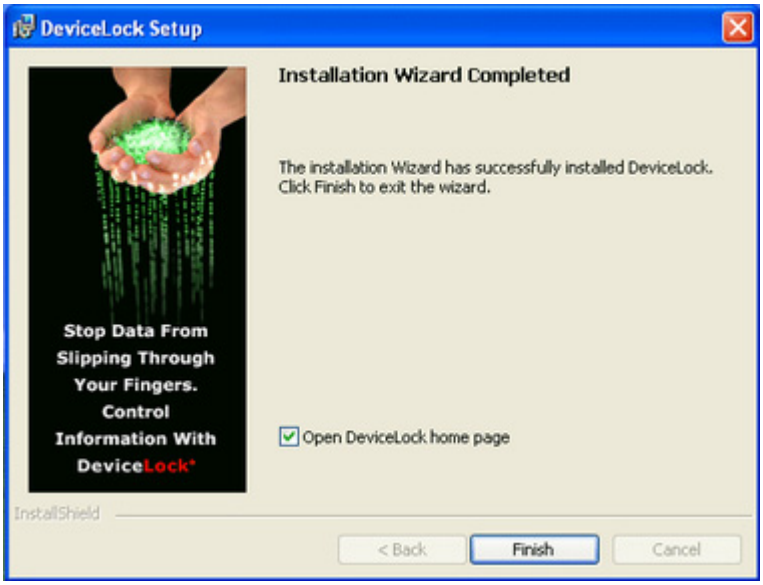
Click **Skip** if you prefer to wait until after installation to set permissions for devices and protocols using DeviceLock management consoles. For more information regarding these settings, please read the Deploying DeviceLock Service section of this manual.

If you opted to install DeviceLock Enterprise Server as well, Setup suggests that you define its settings using the configuration wizard.


DeviceLock Enterprise Server
Log on as
Local System account
This account:
VM2000AD\Administrator
Browse...
Password:
Confirm password:
NOTE: We strongly recommend running DeviceLock Enterprise Server under an account in the Domain Admins group. DeviceLock Enterprise Server must have administrative access to every computer that is trying to connect to it.
Connection settings
Dynamic ports
Fixed TCP port
< Back
Next >
Cancel

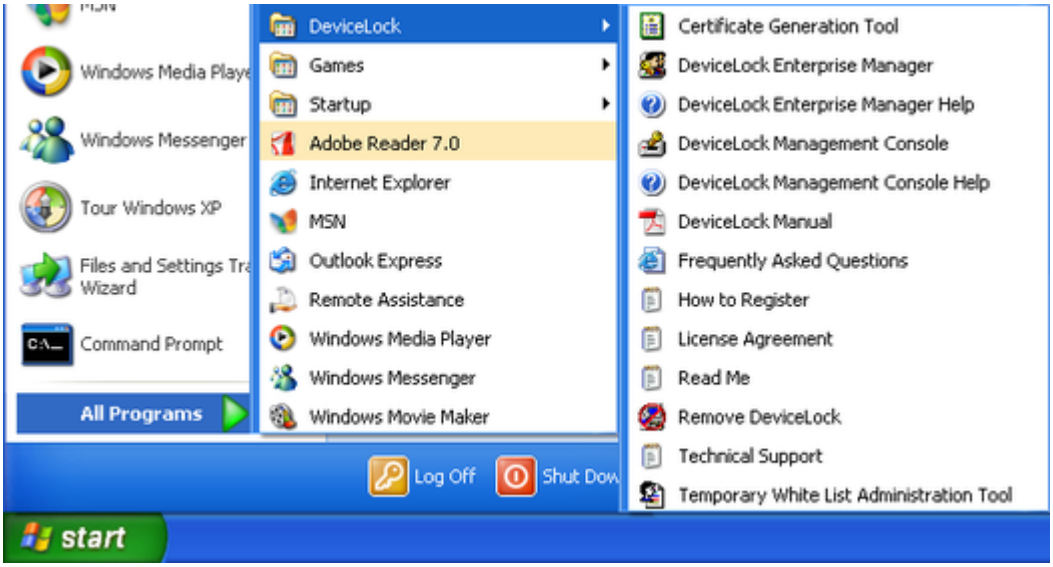
For more information regarding these settings, please read the Installing DeviceLock Enterprise Server section of this manual.

As soon as Setup has installed DeviceLock, it suggests that you point your default Internet browser to the DeviceLock Web site.


DeviceLock Setup
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
Installation Wizard Completed
The installation Wizard has successfully installed DeviceLock. Click Finish to exit the wizard.
Open DeviceLock home page
InstallShield
< Back
Finish
Cancel

Clear the **Open DeviceLock home page** check box if you do not want to visit the DeviceLock Web site. Click **Finish** to finish the installation.

You can locate and run DeviceLock management consoles from the **Programs** menu available by clicking the Windows **Start** button.



Note: DeviceLock Group Policy Manager integrates into Windows Group Policy Editor and is not available as a stand-alone application. In order to use DeviceLock Group Policy Manager, you must run the standard Windows Group Policy Editor.

To uninstall DeviceLock, do one of the following:

Use **Add or Remove Programs** in Control Panel to remove **DeviceLock**.
- OR -
Click **Start**, point to **All Programs**, point to **DeviceLock**, and then click **Remove DeviceLock**.

Installing DeviceLock Enterprise Server

DeviceLock Enterprise Server is the optional component for centralized collection and storage of shadow data and audit logs. Also, DeviceLock Enterprise Server can monitor remote computers in real-time, checking DeviceLock Service status (running or not), policy consistency and integrity.

In order to use DeviceLock Enterprise Server on Windows NT 4.0 SP6 and Windows 2000 computers, you should install Microsoft Data Access Components (MDAC) version 2.8 or later. MDAC is available for free download at the Microsoft Web site: https://www.microsoft.com/en-us/download/details.aspx?id=5793.

Planning Infrastructure

You can install several DeviceLock Enterprise Servers on different computers across your network to uniformly spread the network load.

DeviceLock Enterprise Server uses MS SQL Server to store its data. Hence, it is necessary to have MS SQL Server installed and started in your network before installing DeviceLock Enterprise Server. If you don't have MS SQL Server, you can install the free edition called SQL Server Express Edition available for free download at the Microsoft Web site: http://www.microsoft.com/en-us/server-cloud/Products/sql-server-editions/sql-server-express.aspx.

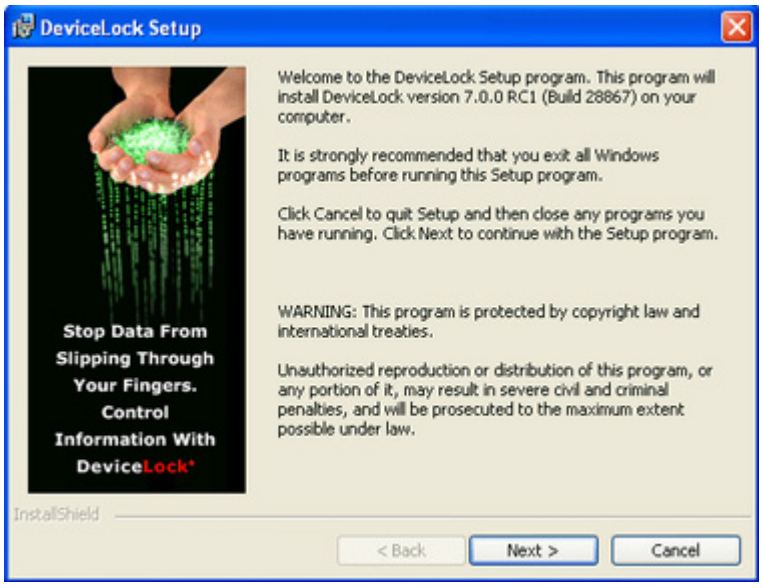
It is not necessary to run MS SQL Server and DeviceLock Enterprise Server on the same machine. Moreover, for performance and reliability reasons, it is better to install DeviceLock Enterprise Server on a separate computer.

There are three scenarios for connecting DeviceLock Enterprise Server and MS SQL Server. You should decide which scenario best fits your needs before installing DeviceLock Enterprise Server:

1. ONE-TO-ONE: you install one DeviceLock Enterprise Server and connect it to one Microsoft SQL Server. This scenario is most appropriate for small networks (up to several hundreds of computers).
2. MANY-TO-MANY: you install several DeviceLock Enterprise Servers and connect each of them to its own Microsoft SQL Server. This scenario is typical for medium and large networks geographically distributed across a variety of segments.
3. MANY-TO-ONE: you install several DeviceLock Enterprise Servers and connect all of them to the one Microsoft SQL Server. This scenario could be used for medium and large networks with a powerful (large amount of memory and free storage space) dedicated machine for Microsoft SQL Server.

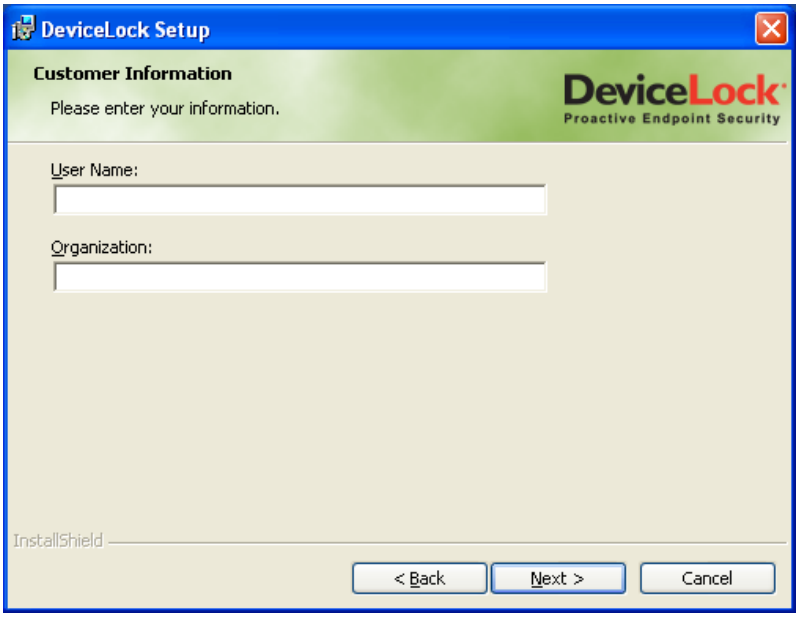
Interactive Installation

Run Setup (**setup.exe**) and follow the instructions that appear on the screen. You must run **setup.exe** on each computer targeted for DeviceLock Enterprise Server installation.


DeviceLock Setup
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
Welcome to the DeviceLock Setup program. This program will install DeviceLock version 7.0.0 RC1 (Build 28867) on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
InstallShield
< Back
Next >
Cancel

You must accept the DeviceLock End User License Agreement before continuing the installation process.

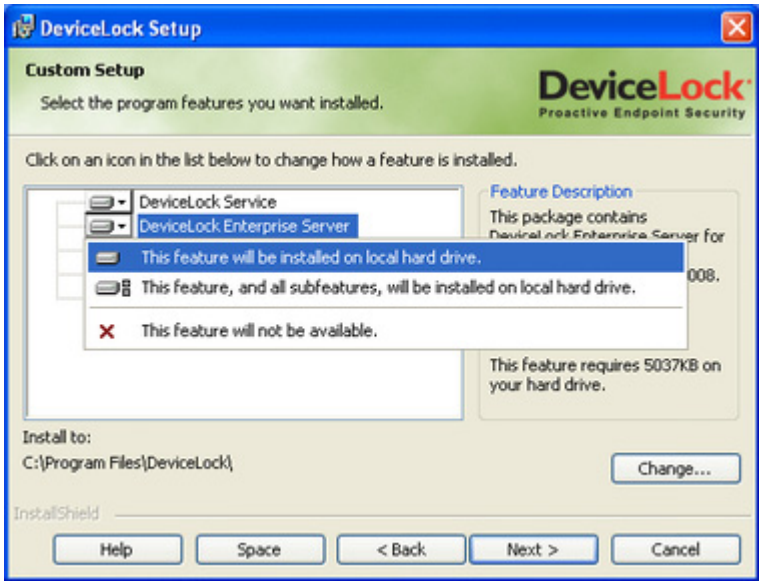
On the **Customer Information** page, type your user name and organization.



On the **Setup type** page, select the required setup type.

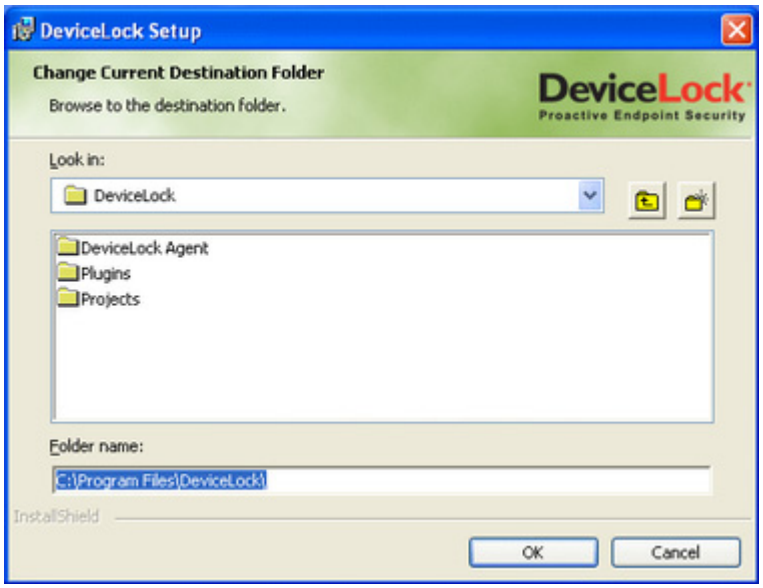
You have the following two choices: either install both DeviceLock Enterprise Server and DeviceLock management consoles using the **Server + Consoles** option or install only DeviceLock Enterprise Server using the **Custom** option and selecting the **DeviceLock Enterprise Server** component.

DeviceLock Setup
Setup Type
Choose the setup type that best suits your needs.
DeviceLock
Proactive Endpoint Security
Please select a setup type.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
Service + Consoles
DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.
Server + Consoles
DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.
InstallShield
< Back
Next >
Cancel

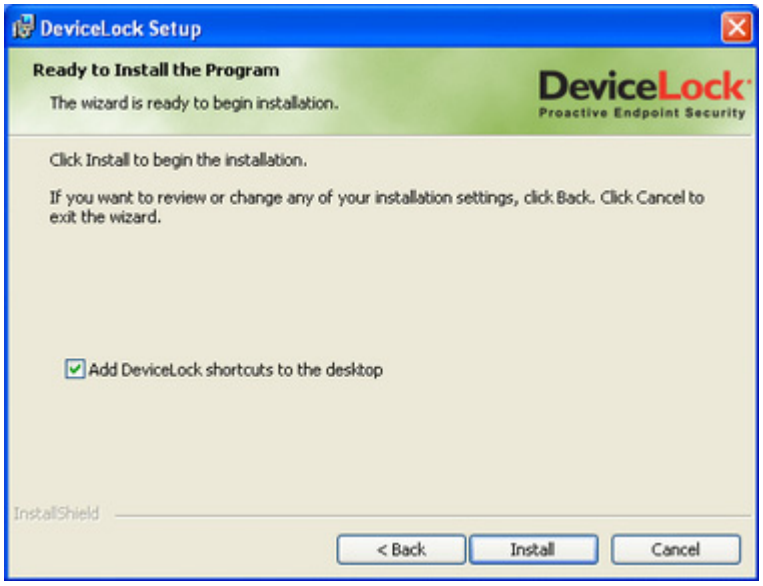

DeviceLock Setup
Custom Setup
Select the program features you want installed.
DeviceLock
Proactive Endpoint Security
Click on an icon in the list below to change how a feature is installed.
DeviceLock Service
DeviceLock Enterprise Server
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
Feature Description
This package contains
This feature requires 5037KB on your hard drive.
Install to:
C:\Program Files\DeviceLock\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

Note: On the **Custom Setup** page, you can select the RSoP component to install. This component enables support for DeviceLock's Resultant Set of Policy planning mode on domain controllers. The RSoP component is required only when DeviceLock management consoles are installed, but DeviceLock Service is not installed on the computer. For more information on RSoP planning mode, refer to the Microsoft documentation.

On the **Custom Setup** page, you can change the default installation directory. By default, the DeviceLock installation directory is **%ProgramFiles%\DeviceLock**. To change the default installation directory, click **Change** to open the **Change Current Destination Folder** page.



On the **Ready to Install the Program** page, click **Install** to begin the installation. Select the **Add DeviceLock shortcuts to the desktop** check box if you want to add DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Service Settings Editor shortcuts to the desktop.

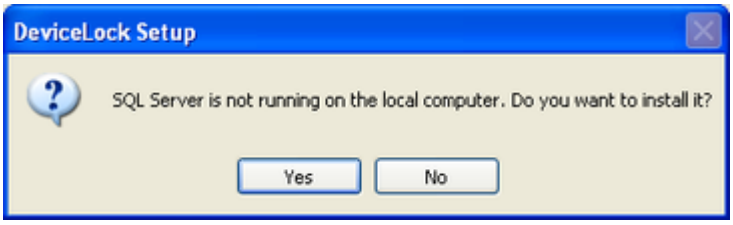

DeviceLock Setup
Ready to Install the Program
The wizard is ready to begin installation.
DeviceLock
Proactive Endpoint Security
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Add DeviceLock shortcuts to the desktop
InstallShield
< Back
Install
Cancel

If you selected to install DeviceLock management consoles as well, Setup may suggest that you generate a new DeviceLock Certificate.

DeviceLock Setup
Do you want to create the new DeviceLock Certificate (the private and public key pair)?
Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.
Yes
No

You can always generate the new DeviceLock Certificate later, using the Certificate Generation Tool installed with DeviceLock management consoles. Hence, if at this step you are not sure whether you need the new certificate or not, just press the **No** button and continue the installation. For more information on DeviceLock Certificates, see "DeviceLock Certificates."

If Setup detects that MS SQL Server is not running on the local computer but its installation package is available, Setup suggests that you run the MS SQL Server installation.



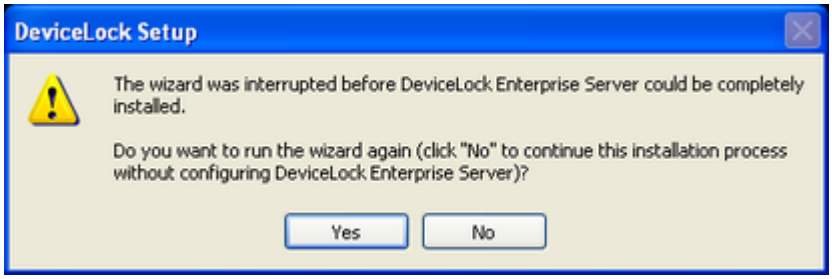
If you don't want to install MS SQL Server on the local computer or it is already installed but just not started, press the **No** button.

During the installation process, you must configure DeviceLock Enterprise Server and define its main settings using the special wizard.

If you are installing an upgrade or just reinstalling DeviceLock Enterprise Server and want to keep its current configuration, you don't need to go through this wizard again – just press the **Cancel** button to close the wizard and keep all existing settings unchanged.

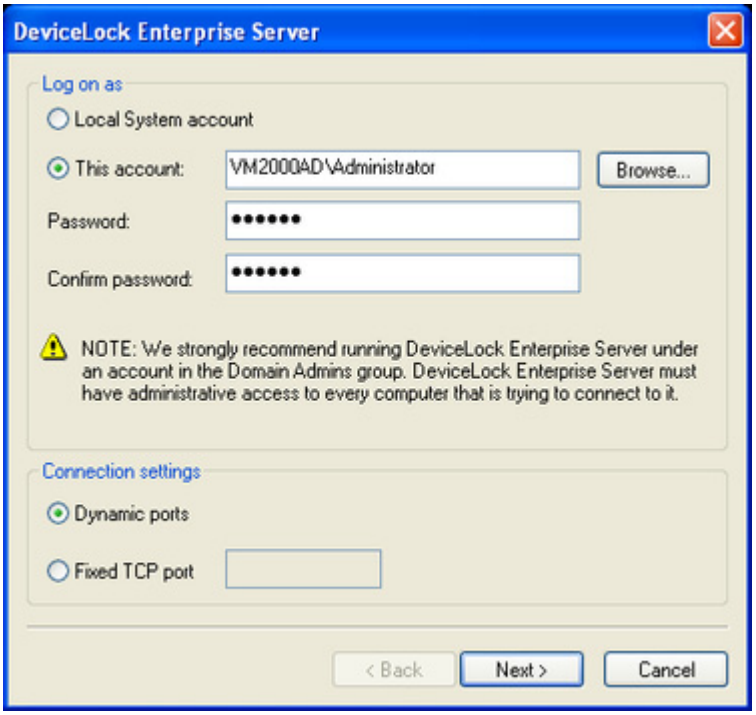
In case you need to change some parameters but keep others – edit only needed parameters and go through all the wizard's pages up to the **Finish** button on the very last page.

Note: If you are installing DeviceLock Enterprise Server for the first time (there are no existing settings on this computer yet) and you cancel the configuration wizard upon opening, Setup will not be able to install DeviceLock Enterprise Server's service, so you'll need to run the configuration wizard again.


DeviceLock Setup
The wizard was interrupted before DeviceLock Enterprise Server could be completely installed.
Do you want to run the wizard again (click "No" to continue this installation process without configuring DeviceLock Enterprise Server)?
Yes
No

If you press the **No** button to continue without installing the DeviceLock Enterprise Server's service, you will need to run Setup later and install the service anyway.

On the first page of the wizard you can opt to install DeviceLock Enterprise Server's service and define its startup parameters.


DeviceLock Enterprise Server
Log on as
Local System account
This account:
VM2000AD\Administrator
Browse...
Password:
Confirm password:
NOTE: We strongly recommend running DeviceLock Enterprise Server under an account in the Domain Admins group. DeviceLock Enterprise Server must have administrative access to every computer that is trying to connect to it.
Connection settings
Dynamic ports
Fixed TCP port
< Back
Next >
Cancel

Log on as

First of all, you should choose an account under which the DeviceLock Enterprise Server's service will start. As many other Windows services, the DeviceLock Enterprise Server's service can start under the special local system account (the SYSTEM user) and on behalf of any user.

To start the service under the SYSTEM user, select the **Local System account** option. Keep in mind that the process working under the SYSTEM user can't access shared network resources and authenticates on remote computers as an anonymous user. Therefore, DeviceLock Enterprise Server configured to run under the SYSTEM user is not able to store shadow files on the remote computer (e.g. on the file

server) and it must use DeviceLock Certificate for authentication on DeviceLock Services running on remote computers.

For more information about authentication methods, please read the description of the Certificate Name parameter.

To start the service on behalf of the user, select the **This account** option, enter the user's account name and the password. It is recommended to use a user account that has administrative privileges on all the computers where DeviceLock Service is running. Otherwise, you will need to use DeviceLock Certificate authentication.

If you're installing DeviceLock Enterprise Server in the domain environment, we recommend that you use a user account that is a member of the Domain Admins group. Since Domain Admins is a member of the local group Administrators on every computer in the domain, members of Domain Admins will have full access to DeviceLock Service on every computer.

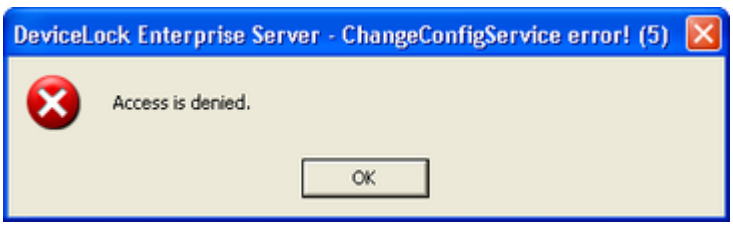
Also, don't forget that if DeviceLock Security is enabled on remotely running DeviceLock Services to protect them against local users with administrative privileges, the user's account specified in the **This account** option must be also in the list of DeviceLock Administrators with **Full access** rights. Otherwise, you'll need to use DeviceLock Certificate authentication.

Connection settings

You can instruct DeviceLock Enterprise Server to use a fixed TCP port for communication with the management console, making it easier to configure a firewall. Type the port number in **Fixed TCP port**. To use dynamic ports for RPC communication, select the **Dynamic ports** option. By default, DeviceLock Enterprise Server is using the 9133 port.

Press the **Next** button to start the DeviceLock Enterprise Server's service and to proceed to the second page.

If the current user doesn't have full administrative access to DeviceLock Enterprise Server (in case it already exists and you're installing an upgrade), the configuration wizard will not be able to install the service and apply changes. Also, the similar error may occur when the current user doesn't have local administrative privileges on the computer where DeviceLock Enterprise Server is installing.



If you've specified an incorrect user name for the **This account** option or the wrong user password, DeviceLock Enterprise Server will not be able to start.

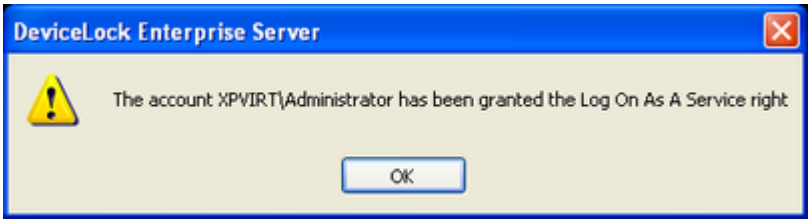
DeviceLock Enterprise Server - ChangeConfigService error! (1057)
The account name is invalid or does not exist, or the password is invalid for the account name specified.
OK

You will be notified if the user's account specified for the **This account** option is not a member of the Domain Admins group.

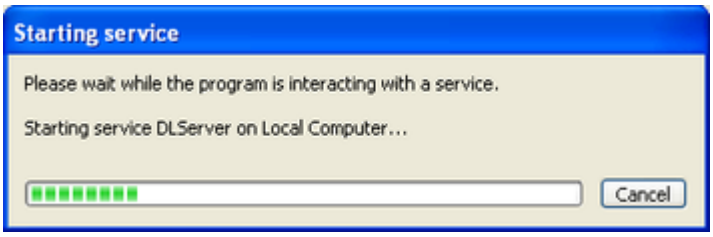
DeviceLock Enterprise Server
The account vm2000ad\test does not belong to the Domain Admins group.
Do you want to continue?
Yes
No

You may continue by pressing the **Yes** button. However keep in mind that in this case either the specified user must have full administrative access to all remotely running DeviceLock Services or DeviceLock Certificate (the public key) must be installed on every computer with DeviceLock Service.

If the user's account specified for the **This account** option doesn't have the Log On As A Service system privilege, the wizard automatically assigns it. This privilege is needed to start the service on behalf of the user.

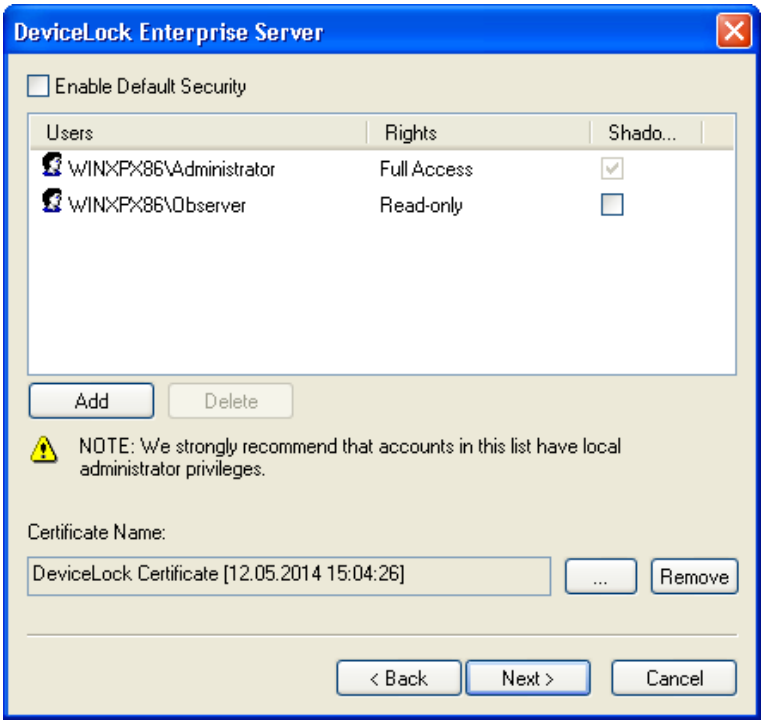


If all of the service's startup parameters were specified correctly, the wizard starts DeviceLock Enterprise Server.


Starting service
Please wait while the program is interacting with a service.
Starting service DLServer on Local Computer...
Cancel

It takes some time (up to a minute) before the DeviceLock Enterprise Server's service is started and the wizard's second page is displayed.

On the second page, you can define the list of users that have administrative access to DeviceLock Enterprise Server and install DeviceLock Certificate (the private key).



Enable Default Security
In the default security configuration all users with local administrator privileges (i.e. members of the local Administrators group) can connect to DeviceLock Enterprise Server using a management console and change its setting and run reports.

To turn on the default security, check the **Enable Default Security** flag.

If you need to define more granular access to DeviceLock Enterprise Server, turn off the default security by unchecking the **Enable Default Security** flag.

Then you need to specify authorized accounts (users and/or groups) that can connect to DeviceLock Enterprise Server. To add a new user or user group to the list of accounts, click on the **Add** button. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the **Delete** button. Using Ctrl and/or Shift you can highlight and remove several records simultaneously.

To define which actions are to be allowed for a user or user group, set the appropriate rights:

- **Full access** – to enable full access to DeviceLock Enterprise Server. Users can change settings and run reports.
- **Change** – to enable change access to DeviceLock Enterprise Server. Users can change settings, install/uninstall DeviceLock Enterprise Server and run reports, but they can't add new users to the list of authorized accounts that can connect to DeviceLock Enterprise Server or change access rights for existing users in this list.
- **Read-only** – to enable only read access to DeviceLock Enterprise Server. Users can run reports and view settings, but can't modify anything.
- **Shadow Data Access** – to enable access to shadowed data. Users can open, view and download shadow data using server's shadow log viewer.

Note: We strongly recommend that accounts included in this list have local administrator privileges because, in some instances, installing, updating and uninstalling DeviceLock Enterprise Server's service may require access rights to Windows Service Control Manager (SCM) and shared network resources.

Certificate Name
You may need to deploy the private key to DeviceLock Enterprise Server if you want to enable authentication based on DeviceLock Certificate.

There are two methods of DeviceLock Enterprise Server authentication on remotely running DeviceLock Services:

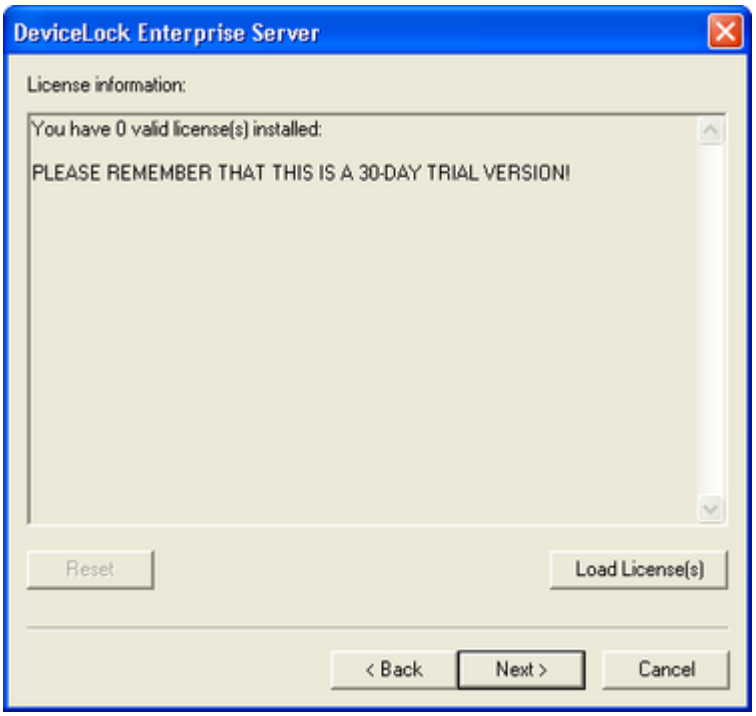
- **User authentication** – the DeviceLock Enterprise Server's service is running under the user's account that has full administrative access to DeviceLock Service on the remote computer. For more information on how to run DeviceLock Enterprise Server on behalf of the user, please read the description of the Log on as parameter.
- **DeviceLock Certificate authentication** – in situations when the user under which DeviceLock Enterprise Server is running can't access DeviceLock Service on the remote computer, you must authenticate based on a DeviceLock Certificate.
  The public key should be installed on DeviceLock Service and the corresponding private key on DeviceLock Enterprise Server.

To install DeviceLock Certificate, press the **...** button, and select the file with a private key. To remove DeviceLock Certificate, press the **Remove** button.

For more information regarding DeviceLock Certificate, please read the DeviceLock Certificates section of this manual.

Press the **Next** button to apply changes and proceed to the third page of the configuration wizard.

From this page, you can load your DeviceLock licenses.



License information
If you've purchased a license for DeviceLock, you should load this license into DeviceLock Enterprise Server.

DeviceLock Enterprise Server handles only the licensed number of DeviceLock Services. For example, if you have a license for 100 computers but there are 101 DeviceLock Services working in your network, DeviceLock Enterprise Server will work with only first 100 DeviceLock Services and ignore the remaining one.

To load the license, press the **Load License(s)** button and select the license file.

You can load several license files in series – one by one.

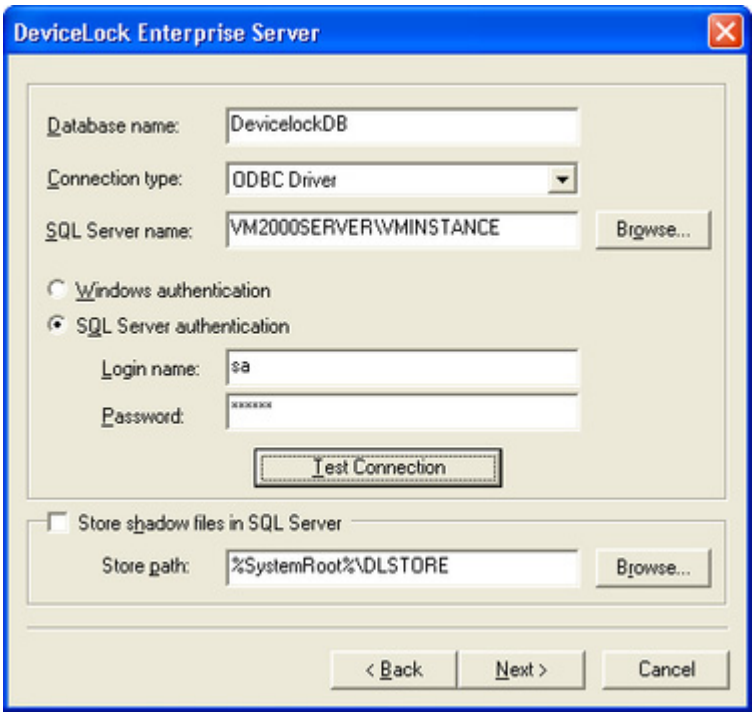
After you have successfully loaded your license files, you can view the license information summary where **Total license(s)** displays the total number of purchased licenses while **Used license(s)** displays the number of licenses currently in use for collection of audit, shadowing and monitoring data on DeviceLock Enterprise Server.

If there are no valid licenses loaded, DeviceLock Enterprise Server works in the trial mode and can handle only two DeviceLock Services.

Note: If a computer with DeviceLock Service leaves the network, DeviceLock Enterprise Server will handle its replacement only after a restart or after 6 hours.

Press the **Next** button to install licenses and proceed to the fourth page.

On the fourth page, you can configure database parameters.



Database name
You must specify the name of the database in SQL Server that will be used to store the DeviceLock Enterprise Server data. The default name suggested by the wizard is **DeviceLockDB**.

Note: You should not create a database with the specified name manually because the configuration wizard creates the database automatically or uses the existing one.

Connection type
There are two ways to define a connection to SQL Server:

1. **ODBC Driver** – you enter the name of SQL Server in **SQL Server name** and select the authentication mode (Windows or SQL Server).

   The **SQL Server name** parameter must contain not just the name of the computer where SQL Server is running but the name of SQL Server itself. Usually the SQL Server name consists of two parts: the computer name and the instance name divided by a backslash (e.g. computer\instance). Sometimes the instance name is empty (default) and you can use the computer name as an SQL Server name. To retrieve SQL Server names available in your local network, press the **Browse** button. (You should have

access to the remote registry of the SQL Server machine to retrieve the instance name.)

If the **SQL Server name** parameter is empty, it means that SQL Server is running on the same computer as DeviceLock Enterprise Server and has an empty (default) instance name.

To establish a connection to SQL Server, you must also configure authentication parameters.

Select the **Windows authentication** option to authenticate on SQL Server under the account used to run DeviceLock Enterprise Server's service.

If the service is running under the SYSTEM user and SQL Server is located on the remote computer, service will not be able to connect to SQL Server since the SYSTEM user doesn't have a right to access the network. For more information on how to run DeviceLock Enterprise Server on behalf of the user, please read the description of the Log on as parameter.

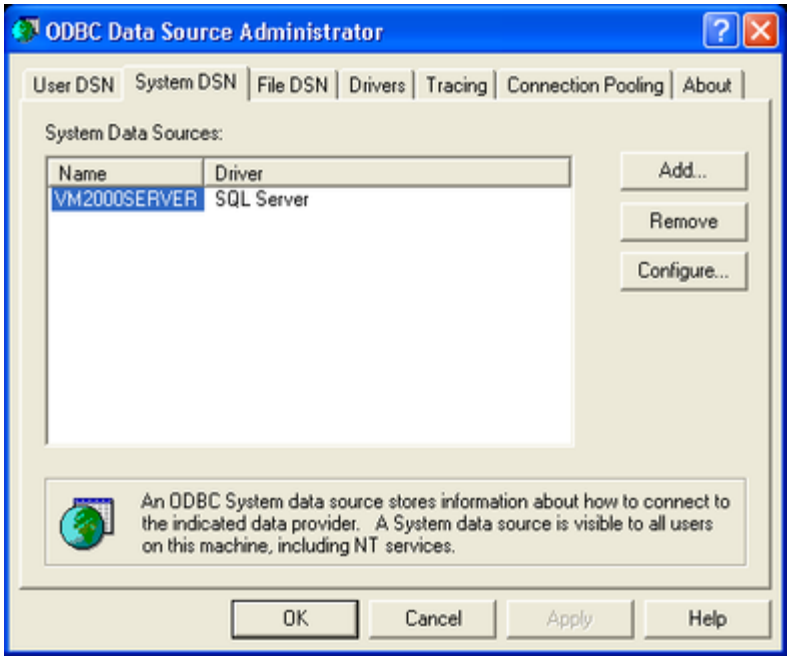
Select the **SQL Server authentication** option to allow SQL Server to perform the authentication itself by checking the login and password previously defined. Before selecting the **SQL Server authentication** option, make sure that your SQL Server was configured to use mixed-mode authentication.

Enter the SQL user name (login) in **Login name** and its password in **Password**.

Note: Windows Authentication is much more secure than SQL Server Authentication. When possible, you should use Windows Authentication.

2. **System Data Source** – you select the predefined system data source from the **Data Source Name** list.

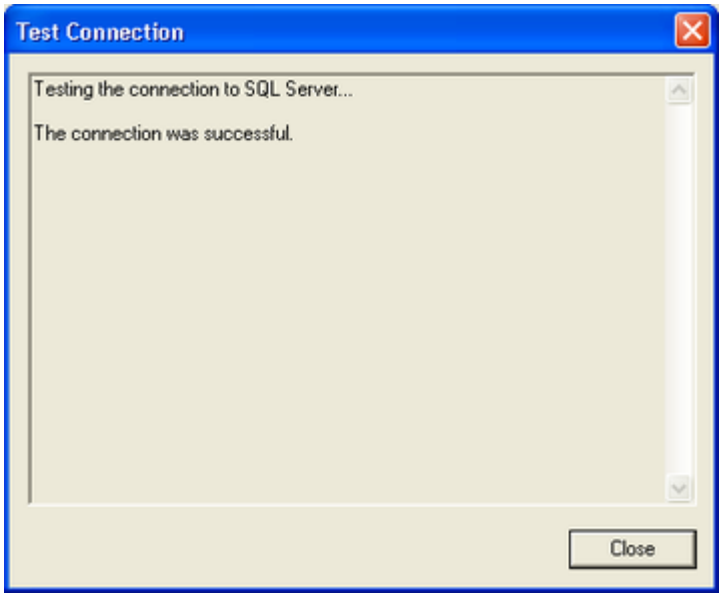
   To define data sources, use the **Data Sources (ODBC**) applet from **Control Panel** -> **Administrative Tools**.



If, in the data source configuration, SQL Server Authentication was chosen, then you also need to specify the SQL user name (login) in **Login name** and its password in **Password**. If Windows Authentication was selected, then you should leave these fields blank.

To refresh the **Data Source Name** list, press the **Refresh** button.

When connection to SQL Server is defined you may want to test it. Press the **Test Connection** button to make sure that all the parameters were specified correctly.



Please note that it only checks connectivity and your access rights to SQL Server. If there are problems with the database or your access rights to this database, you don't see those problems in the **Test Connection** dialog box.

If some connection parameters were specified incorrectly, you may see one of these errors:

- **SQL Server does not exist or access denied** – you've specified an incorrect name of SQL Server in the **SQL Server name** parameter or the remote SQL Server's computer is not accessible. It is possible that you've specified the name of the computer where SQL Server is running but this SQL Server also has an instance name which should be specified as well (e.g. computer\instance).
- **Login failed for user 'COMPUTER_NAME$'** – you've selected Windows Authentication but the user account used to run the DeviceLock Enterprise Server service can't get access to the computer with SQL Server. It may happen when the service starts either under the SYSTEM user or on behalf of a user that doesn't have local administrative privileges on the remote SQL Server's computer.

- **Login failed for user 'user_name'** – you've selected SQL Server Authentication and either specified an incorrect SQL user name (login) or the wrong password for it. Please note that SQL users are different from Windows users and you can't use the regular Windows account in the **Login name** parameter. SQL users exist only in SQL Server and to manage them you should use SQL Server management consoles (such as Microsoft SQL Server Management Studio).
- **Login failed for user 'user_name'. The user is not associated with a trusted SQL Server connection** – you've selected SQL Server Authentication but your SQL Server doesn't support this mode. You should either use Windows Authentication or allow your SQL Server to work in the mixed mode (SQL Server and Windows Authentication mode).
- **Login failed for user ''. The user is not associated with a trusted SQL Server connection** – the data source you've specified in **Data Source Name** was configured to use the SQL Server Authentication mode but the **Login name** parameter is empty.
- **Data source name not found and no default driver specified** – you've selected **System Data Source** from the **Connection type** list and specified either an empty or non-existent name in **Data Source Name**.

Store shadow files in SQL Server

There are two modes of storing binary data: data can be stored in SQL Server or it can be stored on the disk.

To store data in SQL Server, check the **Store shadow files in SQL Server** flag.

If you decided to store binary data in SQL Server, we recommend that you dramatically increase the maximum file size parameter for the transaction log of the database specified in **Database name**. Otherwise, SQL Server may fail to handle the large amount of data (hundreds of megabytes) in one transaction. Also, it is recommended that you increase the maximum amount of memory available for SQL Server and turn on the PAE (Physical Address Extension) feature.

For more information on how to tune up your SQL Server for storing large amounts of data, please read the article available at the Microsoft Web site: http://technet.microsoft.com/en-us/library/cc966420.aspx.

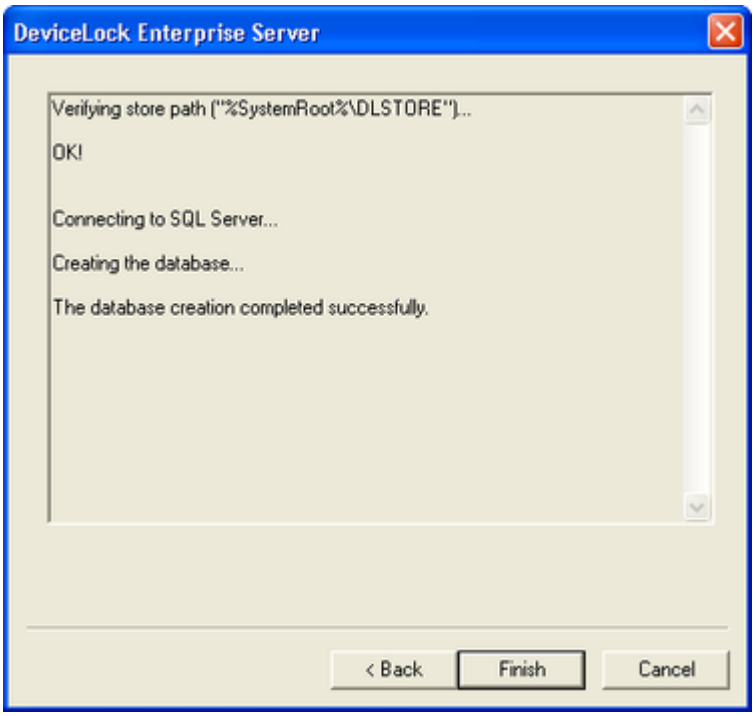
To store data on the disk, uncheck the **Store shadow files in SQL Server** flag. In this case only links to the binary data and some additional information are stored in SQL Server.

When stored on the disk, data files are located by the path specified in the **Store path** parameter. To choose the folder where files should be stored, you can use the **Browse** button.

You can also specify the network shared resource (e.g. \\server\dlstore) that will be used as storage. Make sure that the user account used to run the DeviceLock Enterprise Server service has full access to this network resource.

Note: It is recommended to store binary data on the disk.

Press the **Next** button to apply changes and proceed to the last page.



It takes some time to create the database specified in **Database name** if it does not exist on this SQL Server yet. If the database already exists and it has the proper format (i.e. was created by DeviceLock Enterprise Server) then DeviceLock Enterprise Server keeps all existing data and uses this database.

Note: If necessary, DeviceLock automatically updates the database to the latest version.

If some parameters on the previous wizard's page were specified incorrectly, you may see one of these errors:

- **[2] The system cannot find the file specified** – you've configured DeviceLock Enterprise Server to store binary data on the disk but the path specified in **Store path** is incorrect. If you've specified the shared network resource then it is possible that this network resource is not accessible.
- **Failed to verify store path. [5] Access is denied** – the path specified in the **Store path** parameter is correct, but the user account used to run the DeviceLock Enterprise Server service doesn't have full access to files by this path.

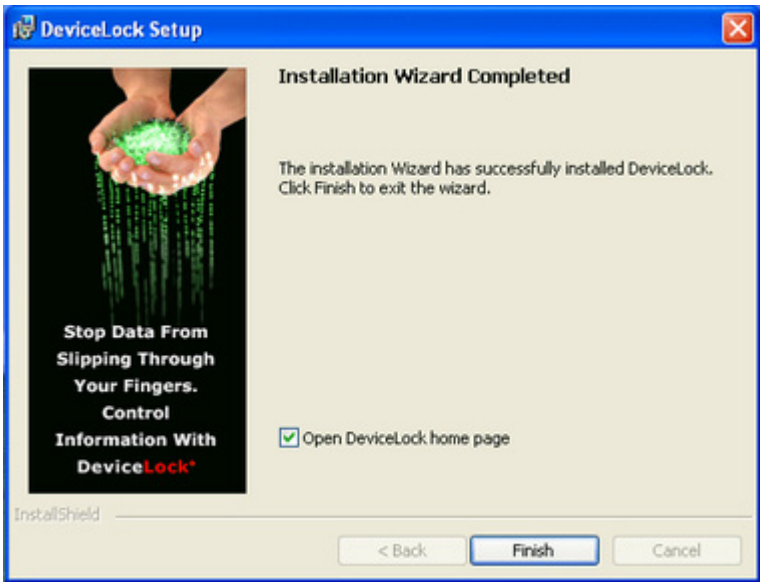
- **CREATE DATABASE permission denied in database 'name'** – the user's account (login) used to connect to SQL Server doesn't have enough privileges to create the database. The login should have at least the dbcreator Server role (see **Server Roles** in **Login Properties** of Microsoft SQL Server Management Studio).
- **The server principal "user_name" is not able to access the database "name" under the current security context** – the user's account (login) used to connect to SQL Server doesn't have access to the existing database. The login should be mapped to this database (see **User Mapping** in **Login Properties** of Microsoft SQL Server Management Studio).
- **SELECT permission denied on object 'name', database 'name', schema 'name'** – the user's account (login) used to connect to SQL Server doesn't have read/write access to the existing database. The login should have at least db_datareader and db_datawriter Database roles (see **User Mapping** in **Login Properties** of Microsoft SQL Server Management Studio).
- **Invalid object name 'name'** – the database specified in the **Database name** parameter already exists in this SQL Server but has an incorrect format. It happens when you are trying to use the database that was not created by DeviceLock Enterprise Server or if the database was corrupted.
- **DeviceLock Database has an unsupported format** – the database specified in the **Database name** parameter already exists but is outdated. This existing database has an unsupported format so it can't be automatically upgraded to the new format. You should either use another database or create a new one.
- **DeviceLock Database has a format that is not supported by the current server version** – the database specified in the **Database name** parameter already exists but it was created by the more recent version of DeviceLock Enterprise Server. You should either use the latest version of DeviceLock Enterprise Server or use another database (or create a new one).

Also, some of the SQL Server connection errors described above may be displayed here as well.

Use the **Back** button to return to the previous page of the wizard and make necessary changes.

If there are no errors, press the **Finish** button to close the wizard and continue the installation process.

As soon as Setup has installed DeviceLock, it prompts you to point your default Internet browser to the DeviceLock Web site.



Clear the **Open DeviceLock home page** check box if you do not want to visit the DeviceLock Web site. Click **Finish** to finish the installation.

Note: To uninstall DeviceLock, do one of the following:

Use **Add or Remove Programs** in Control Panel to remove **DeviceLock**.
- OR -
Click **Start**, point to **All Programs**, point to **DeviceLock**, and then click **Remove DeviceLock**.

Installing and Accessing DeviceLock WebConsole

DeviceLock WebConsole provides a simple and intuitive Web interface for DeviceLock Management Console and DeviceLock Service Settings Editor. With DeviceLock WebConsole, you are not limited to managing DeviceLock Service, DeviceLock Enterprise Server and DeviceLock Content Security Server from a particular machine where DeviceLock Management Console and DeviceLock Service Settings Editor have been installed. Instead, you can access and use DeviceLock WebConsole from any supported Web browser.

DeviceLock WebConsole is not installed by default. Follow these steps to install and access DeviceLock WebConsole:

- Step 1. Prepare for the installation
- Step 2. Install DeviceLock WebConsole
- Step 3. Access DeviceLock WebConsole

Step 1. Prepare for the installation

Before you install DeviceLock WebConsole, consider the following important notes:

- The computer on which you install DeviceLock WebConsole must meet the following system requirements:

Operating System	Microsoft Windows XP/Vista/7/8/8.1/10 and Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2. Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
RAM	Minimum: 512 MB.
Hard Disk Space	Minimum:230 MB.
Other Prerequisites	Before installing DeviceLock WebConsole, you must download and install the .NET Framework 3.5 SP 1.

- You must have administrator permissions to install DeviceLock WebConsole.
- Use one of the following browsers with DeviceLock WebConsole: Microsoft Internet Explorer; Mozilla Firefox; Google Chrome; Apple Safari; Opera.

  Note: It is highly recommended that you use the latest browser versions.

- We strongly recommend that you exit all Windows programs before you start Setup.

Step 2. Install DeviceLock WebConsole

DeviceLock WebConsole can be installed either via the **Custom** setup option or silently.

Use this procedure to install DeviceLock WebConsole using the Setup program.

To install DeviceLock WebConsole using the Setup program

1. Open the DeviceLock.zip file, and then double-click the **setup.exe** file to start the Setup program.
2. Follow the instructions in the Setup program.
3. On the **License Agreement** page, read the License Agreement and then click **I accept the terms in the license agreement** to proceed with the installation.
4. On the **Customer Information** page, type your user name and organization, and then click **Next**.
5. On the **Setup Type** page, select the **Custom** option, and then click **Next**.
6. On the **Custom Setup** page, click the drop-down arrow next to **DeviceLock WebConsole**, and then click **This feature, and all subfeatures, will be installed on local hard drive**. Click **Next**.

   On this page, you can change the default installation directory. By default, the DeviceLock WebConsole installation directory is %ProgramFiles%\DeviceLock\Web. To change the default installation directory, click Change to open the Change Current Destination Folder page.

During installation, Setup installs and configures Apache HTTP Server as the Web server for DeviceLock WebConsole. By default, the Apache HTTP Server installation directory is %ProgramFiles%\DeviceLock\Web\Apache2.

7. On the **Web Server Settings** page, configure the Web server, and then click **Next**. To configure the Web server, use the following settings:
   - **Port** – specifies the port on which the Web server listens for HTTP requests from the Web browser. The default is **80**.
     Make sure the specified port is open.
   - **Enable SSL communication** – enables SSL security on the Web server.
   - **SSL port** – specifies the port on which the Web server listens for HTTPS requests from the Web browser. The default is **443**.
   - **Server name** – specifies the Web server's host name.
   - **SSL key file path** – specifies the full path to the SSL key file. Click the ellipsis button ... to select the file.
   - **SSL certificate file path** – specifies the full path to the SSL certificate file. Click the ellipsis button ... to select the file.
8. **On the Ready to Install the Program** page, click **Install**.
9. On the **Installation Wizard Completed** page, click **Finish** to complete the installation.

   On this page, you will have the option to go to the DeviceLock home page. This option is selected by default.

Note: To uninstall DeviceLock WebConsole, do one of the following:

Use **Add or Remove Programs** in Control Panel to remove **DeviceLock**.
- OR -
Click **Start**, point to **All Programs**, point to **DeviceLock**, and then click **Remove DeviceLock**.

You can also install DeviceLock WebConsole silently from the command line. To perform a silent installation, use the command: setup.exe /s and the devicelock.ini file with installation settings. The devicelock.ini file is supplied with DeviceLock in the DeviceLock.zip file. The devicelock.ini file is used to specify silent installation parameters. You can open and edit devicelock.ini in any text editor, for example in Notepad to customize an installation. Remove a semicolon (;) before the parameter to assign a new value or leave it to assign the default value. The devicelock.ini file must be in the same directory as setup.exe. The devicelock.ini file contains the following parameters for unattended installations of DeviceLock WebConsole:

PARAMETER	DESCRIPTION
WebConsole	Installs DeviceLock WebConsole and Apache Web Server. Possible values: **0** and **1**. To install DeviceLock WebConsole and Apache Web Server, set the **WebConsole** parameter to **1**. The default value is **0**.

PARAMETER	DESCRIPTION
Port	Specifies the port on which the Web server listens for HTTP requests from the Web browser. The default value is **80**.
ServerName	Specifies the Web server's host name.
SSLPort	Specifies the port on which the Web server listens for HTTPS requests from the Web browser. The default value is **443**.
SSLKeyFile	Specifies the full path to the SSL key file.
SSLCertFile	Specifies the full path to the SSL certificate file.

For more information on SSL/TLS, please refer to:
http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html.

For detailed information on unattended installation and other available parameters in the devicelock.ini file, see "Unattended installation."

Step 3. Access DeviceLock WebConsole

When the installation completes successfully, you can access and use DeviceLock WebConsole.

To access DeviceLock WebConsole through your Web browser

1. Enter one of the following URLs:

   http://<*your_console_host*>:<*http_port*>

   - OR –

   https://<*your_console_host*>:<*https_port*>

   where:

   <*your_console_host*> is the IP address or DNS name of the computer where DeviceLock WebConsole is installed. If you are running the browser on the computer on which DeviceLock WebConsole is installed, replace <*your_console_host*> with **localhost**.

   <*http_port*> is the port number used to access DeviceLock WebConsole using an unsecure connection over HTTP. <*http_port*> may be omitted if the default port 80 is used.

   <*https_port*> is the port number used to access DeviceLock WebConsole using a secure connection over HTTPS. <*https_port*> may be omitted if the default port 443 is used.

2. When prompted, log in to DeviceLock WebConsole using the administrator user ID and password.

Procedures for defining policies via DeviceLock WebConsole are similar to procedures for defining policies via DeviceLock Management Console and DeviceLock Service Settings Editor. For more information, see "DeviceLock Management Console" and "DeviceLock Service Settings Editor."

Installing DeviceLock Content Security Server

The DeviceLock Content Security Server package consists of Search Server and Discovery Server. Follow these steps to install DeviceLock Content Security Server:

- Step 1. Prepare for the installation
- Step 2. Start the installation
- Step 3. Configure DeviceLock Content Security Server and complete the installation.

Step 1. Prepare for the installation

Before you install DeviceLock Content Security Server, consider the following important notes:

- The computer on which you install DeviceLock Content Security Server must meet the following system requirements:

Operating System	Microsoft Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2. Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
SQL Server	Microsoft SQL Server 2005 or later must be installed. **Note:** Microsoft SQL Server is only required if you are planning to use DeviceLock Discovery Server. If you are not planning to make use of Discovery Server, you don't have to install SQL Server.
Hard Disk Space	Minimum:1 GB. Recommended: 800 GB (if an SQL database is used).

- You must have administrator permissions to install DeviceLock Content Security Server.
- For optimal performance and reliability, we recommend that you install DeviceLock Enterprise Server and DeviceLock Content Security Server on different computers.
- There is a special Search Server license which you must purchase for DeviceLock Content Security Server. You can use the same license on an unlimited number of computers running DeviceLock Content Security Server. The Search Server licensing model is based on the number of log entries to be indexed for full-text search. Each license allows Search Server to index 1,000 entries from the shadow logs (Shadow Log and Deleted Shadow Data Log), and 5,000 entries from every other log (Audit Log, Server Log, and Monitoring Log). Depending on the actual number of log entries on your DeviceLock Enterprise Servers, you can purchase as many licenses as required. If you use several licenses for Search Server, it can index as many log entries as the combined licenses allow. The trial period for DeviceLock Content Security

Server is 30 days. During the trial period, Search Server can index 2,000 entries from the shadow logs and 10,000 entries from every other log.

- There is a special DeviceLock Discovery license which you must purchase for DeviceLock Content Security Server. A license is required for each computer or network device scanned with DeviceLock Discovery, regardless of whether the system is set to scan the entire computer or a single folder. The trial period for DeviceLock Discovery is 30 days. The maximum of two computers can be scanned with the evaluation version.
- In case you have several DeviceLock Enterprise Servers on your network, you can also install several DeviceLock Content Security Servers to spread the load. However, this approach only makes sense if all these DeviceLock Enterprise Servers are not connected to the same Microsoft SQL Server (i.e. not in the "MANY-TO-ONE" mode).
- When you have several DeviceLock Content Security Servers installed each Search Server will have its own search index. Hence, you have to connect to every DeviceLock Content Security Server and run the same search queries on every Search Server in order to get the complete result set from all the data stored on all DeviceLock Enterprise Servers.
- There are two scenarios for connecting DeviceLock Discovery Server and MS SQL Server. You should decide which scenario best fits your needs before installing the product. DeviceLock Discovery Server supports ONE-TO-ONE and MANY-TO-MANY modes:
  1. **ONE-TO-ONE**: you install one DeviceLock Content Security Server and connect it to one Microsoft SQL Server. This scenario is most appropriate for small networks (up to several hundreds of computers).
  2. **MANY-TO-MANY**: you install several DeviceLock Content Security Servers and connect each of them to its own Microsoft SQL Server. This scenario is typical for medium and large networks geographically distributed across a variety of segments.
- We strongly recommend that you exit all Windows programs before you start Setup.

Step 2. Start the installation

Use this procedure to begin the installation process.

To start the installation

1. Open the **DeviceLock.zip** file, and then double-click the **setup_dlcss.exe** file to start the Setup program.

   You must run the Setup program on each computer on which you want to install DeviceLock Content Security Server.

2. Follow the instructions in the Setup program.

3. On the **License Agreement** page, read the License Agreement and then click **I accept the terms in the license agreement** to accept the licensing terms and conditions and proceed with the installation.
4. On the **Customer Information** page, type your user name and organization, and then click **Next**.
5. On the **Destination Folder** page, accept the default installation location or click **Change** to modify the path as needed. Click **Next**.

   The default installation directory is %ProgramFiles%\DeviceLock Content Security Server.

6. On the **Ready to Install the Program** page, click **Install** to begin the installation.

   The DeviceLock Content Security Server wizard starts.

   If you are installing an upgrade or just re-installing DeviceLock Content Security Server and want to keep its current configuration, you do not need to go through this wizard again – just click **Cancel** to close the wizard and keep all existing settings unchanged.

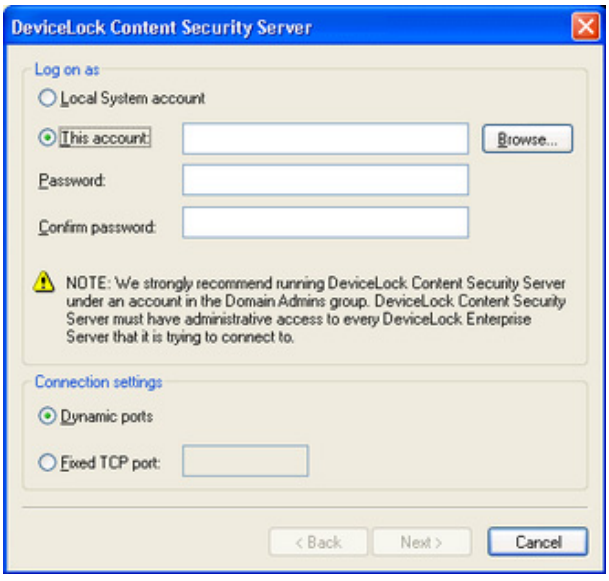
   In case you need to change some parameters but keep others – edit only needed parameters and go through all the wizard's pages up to the **Finish** button on the final page.

Note: If you are installing DeviceLock Content Security Server for the first time (there are no existing settings on this computer yet) and you cancel the configuration wizard upon opening, Setup will not be able to install DeviceLock Content Security Server's service, so you will need to run the configuration wizard again.

Step 3. Configure DeviceLock Content Security Server and complete the installation

The DeviceLock Content Security Server wizard opens automatically during the installation process. This wizard will guide you through the required settings you must configure to use DeviceLock Content Security Server.

The first page of the wizard looks like this:


DeviceLock Content Security Server
Log on as
Local System account
This account:
Browse...
Password:
Confirm password:
NOTE: We strongly recommend running DeviceLock Content Security Server under an account in the Domain Admins group. DeviceLock Content Security Server must have administrative access to every DeviceLock Enterprise Server that it is trying to connect to.
Connection settings
Dynamic ports
Fixed TCP port:
< Back
Next >
Cancel

On this page, you configure startup options for the DeviceLock Content Security Server service.

Log on as
First of all, you should choose an account under which the DeviceLock Content Security Server service will start. As with many other Windows services, the DeviceLock Content Security Server service can start under the special local system account (the SYSTEM user) and on behalf of any user.

To start the service under the SYSTEM user, select the **Local System account** option. Keep in mind that the process working under the SYSTEM user cannot access shared network resources and authenticates on remote computers as an anonymous user. Therefore, DeviceLock Content Security Server configured to run under the SYSTEM user is not able to access DeviceLock Enterprise Server running on the remote computer and it must use DeviceLock Certificate for authentication on it.

For more information about authentication methods, please read the description of the Certificate Name parameter.

To start the service on behalf of the user, select the **This account** option, enter the user's account name and the password. It is recommended to use a user account that has administrative privileges on all the computers where DeviceLock Enterprise Server is running. Otherwise, you will need to use DeviceLock Certificate authentication.

If you are installing DeviceLock Content Security Server in the domain environment, we recommend that you use a user account that is a member of the Domain Admins group. Since Domain Admins is a member of the local group Administrators on every computer in the domain, members of Domain Admins will have full access to every computer.

Also, do not forget that if Default Security is disabled on:

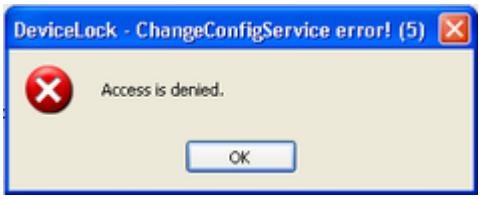
- remotely running DeviceLock Enterprise Server, the user's account specified in the **This account** option must be also in the list of Server Administrators with at least **Read-only** access rights on that DeviceLock Enterprise Server. Otherwise, you will need to use DeviceLock Certificate authentication.

- remotely running DeviceLock Service, the user's account specified in the **This account** option must be also in the list of DeviceLock Administrators with at least **Read-only** access rights on that DeviceLock Service. Otherwise, you will need to use DeviceLock Certificate authentication or specify credentials in the corresponding DeviceLock Discovery unit.

Connection settings
You can instruct DeviceLock Content Security Server to use a fixed TCP port for communication with the management console, making it easier to configure a firewall. Type the port number in **Fixed TCP port**. To use dynamic ports for RPC communication, select the **Dynamic ports** option. By default, DeviceLock Content Security Server uses port 9134.

Click **Next** to start the DeviceLock Content Security Server service and to proceed to the second page.

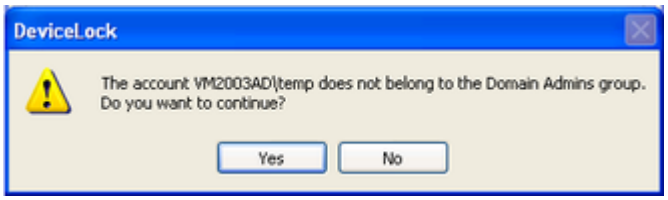
If the current user does not have full administrative access to DeviceLock Content Security Server (in case it already exists and you're installing an upgrade), the configuration wizard will not be able to install the service and apply changes. Also, a similar error may occur when the current user does not have local administrative privileges on the computer where DeviceLock Content Security Server is installing.



If you have specified an incorrect user name for the **This account** option or the wrong user password, DeviceLock Content Security Server will not be able to start.

DeviceLock - ChangeConfigService error! (1057)
The account name is invalid or does not exist, or the password is invalid for the account name specified.
OK

You will be notified if the user's account specified for the **This account** option is not a member of the Domain Admins group.



You may continue by clicking **Yes**. However, make sure that either of the following is true.

For Search Server:

- The specified user must have administrative access to all remotely running DeviceLock Enterprise Servers;

  - OR -

- DeviceLock Certificate (the private key) must be installed on every computer with DeviceLock Enterprise Server.

For DeviceLock Discovery Server:

- The specified user must have administrative access to all computers scanned by DeviceLock Discovery Server. This includes computers that are running DeviceLock Services, DeviceLock Discovery Agents, as well as any computers not having the Agent installed;

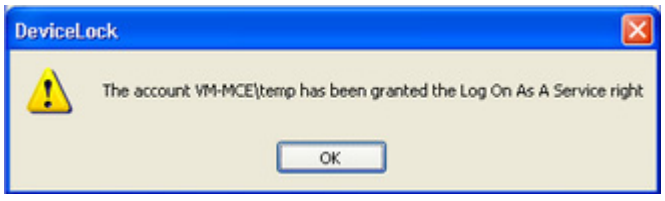
  - OR -

- DeviceLock Certificate (the public key) must be installed on every computer (with DeviceLock Service) scanned by DeviceLock Discovery Server;

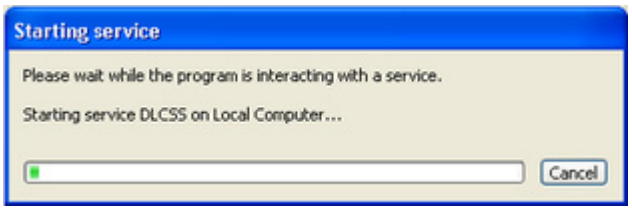
  - OR –

- Credentials for accessing remote computers must be specified in the scanning settings.

If the user's account specified for the **This account** option does not have the Log On As A Service system privilege, the wizard automatically assigns it. This privilege is needed to start the service on behalf of the user.

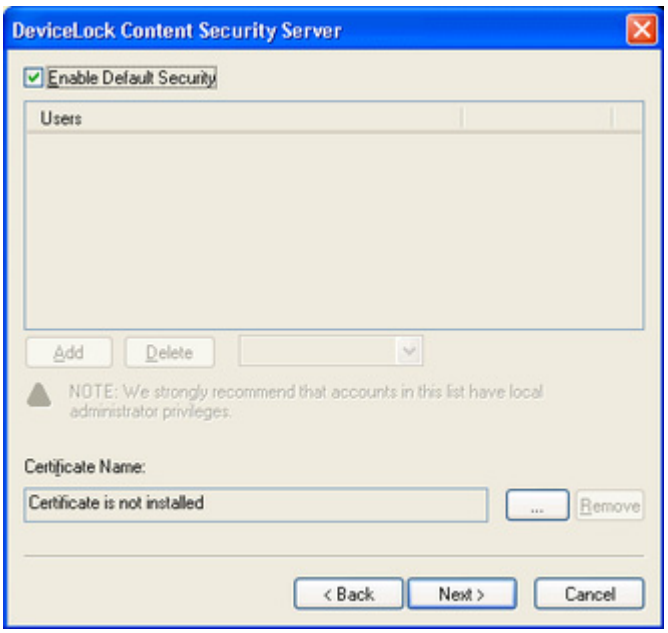


If all of the service's startup parameters were specified correctly, the wizard starts DeviceLock Content Security Server.


Starting service
Please wait while the program is interacting with a service.
Starting service DLCSS on Local Computer...
Cancel

It takes some time (up to a minute) before the DeviceLock Content Security Server service is started and the wizard's second page is displayed.

The second page of the wizard looks like this.



On this page, you define the list of users that have administrative access to DeviceLock Content Security Server and install DeviceLock Certificate (the private key).

Enable Default Security

In the default security configuration all users with local administrator privileges (i.e. members of the local Administrators group) can connect to DeviceLock Content Security Server using a management console, change its settings, run search queries, configure content detection settings, and run discovery tasks.

To turn on the default security, select the **Enable Default Security** check box.

If you need to define more granular access to DeviceLock Content Security Server, turn off the default security by clearing the **Enable Default Security** check box.

Then you need to specify authorized accounts (users and/or groups) that can connect to DeviceLock Content Security Server. To add a new user or group to the list of accounts, click **Add**. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the **Delete** button. Using Ctrl and/or Shift you can highlight and remove several records simultaneously.

To define which actions are to be allowed for a user or user group, set the appropriate rights:

- **Full access** – enables full access to DeviceLock Content Security Server. Users can install/uninstall DeviceLock Content Security Server, connect to it using DeviceLock Management Console, change its settings, run search queries, configure content detection settings, and run discovery tasks.
- **Change** – enables change access to DeviceLock Content Security Server. Users can install/uninstall DeviceLock Content Security Server, connect to it using DeviceLock Management Console, change its settings, run search queries, configure content detection settings, and run discovery tasks; but they cannot add and remove users to and from the Server Administrators group or change access rights granted to Server Administrators.
- **Read-only** – enables read-only access to DeviceLock Content Security Server. Users can connect to DeviceLock Content Security Server using DeviceLock Management Console, run search queries, view settings and discovery reports; but they cannot modify any settings, run a discovery task, or create a new index for the Search Server.
- **Shadow Data Access** - to enable access to shadowed data. Users can open, view and download shadow data on search results page and search inside of shadowed files.

Note: We strongly recommend that accounts included in this list have local administrator privileges because, in some instances, installing, updating and uninstalling the DeviceLock Content Security Server service may require access rights to Windows Service Control Manager (SCM) and shared network resources.

Certificate Name

You may need to deploy the private key to DeviceLock Content Security Server if you want to enable authentication based on DeviceLock Certificate.

There are two methods of DeviceLock Search Server authentication on a remotely running DeviceLock Enterprise Server:

- **User authentication** – the DeviceLock Content Security Server service is running under the user's account that has administrative access to DeviceLock Enterprise Server on the remote computer. For more information on how to

run DeviceLock Content Security Server on behalf of the user, please read the description of the Log on as parameter.

- **DeviceLock Certificate authentication** – in situations when the user under which DeviceLock Content Security Server is running cannot access DeviceLock Enterprise Server on the remote computer, you must authenticate based on a DeviceLock Certificate.

  The same private key should be installed on DeviceLock Enterprise Server and on DeviceLock Content Security Server.

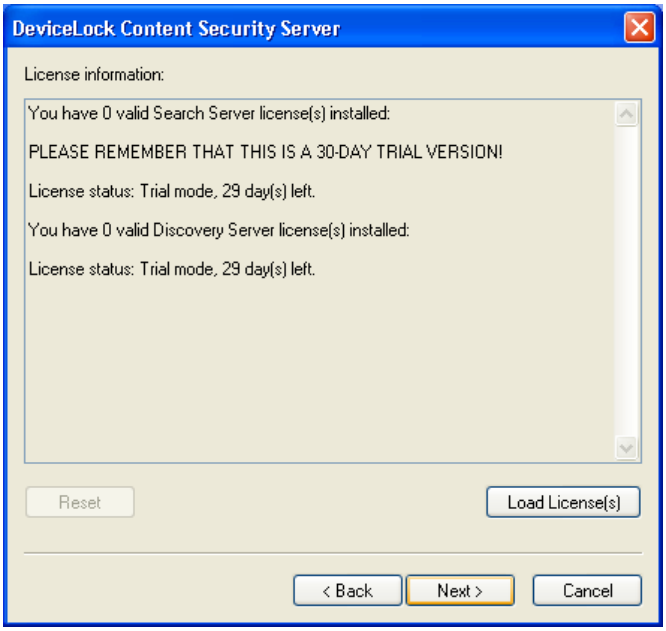
There are three methods of DeviceLock Discovery Server authentication when scanning a remote computer:

- **User authentication** – the DeviceLock Content Security Server service is running under a certain user account, and these credentials are used to access remote computers being scanned. These credentials will be supplied to either DeviceLock Service, DeviceLock Discovery Agent, or the remote computer if scanning is performed without an agent. For more information on how to run DeviceLock Content Security Server on behalf of a user, please read the description of the Log on as parameter.
- **Alternative credentials authentication** – the DeviceLock Content Security Server service is running under a user account that has administrative privileges at least on the local computer. DeviceLock Discovery Server will use alternative credentials to log in to remote computer being scanned.
- **DeviceLock Certificate authentication** – authentication based on a DeviceLock Certificate is used to authorize on remote computers running DeviceLock Service and having the corresponding public certificate installed.

To install DeviceLock Certificate, click the ellipsis button , and select the file with a private key. To remove DeviceLock Certificate, click **Remove**.

For more information regarding DeviceLock Certificate, see "DeviceLock Certificates."

Click **Next** to apply changes and proceed to the next page of the configuration wizard.


DeviceLock Content Security Server
License information:
You have 0 valid Search Server license(s) installed:
PLEASE REMEMBER THAT THIS IS A 30-DAY TRIAL VERSION!
License status: Trial mode, 29 day(s) left.
You have 0 valid Discovery Server license(s) installed:
License status: Trial mode, 29 day(s) left.
Reset
Load License(s)
< Back
Next >
Cancel

On this page, you can load your licenses.

License information
If you have purchased a license for Search Server and/or DeviceLock Discovery, you should load this license into DeviceLock Content Security Server.

To load the license, click **Load License(s)** and select the license file. You can load several license files in series – one by one.

After you have successfully loaded your license files, you can view the license information summary where **Total license(s)** displays the total number of purchased licenses while **Used license(s)** displays the number of licenses currently in use either for indexing of textual log data on DeviceLock Enterprise Server or for scanning with DeviceLock Discovery.

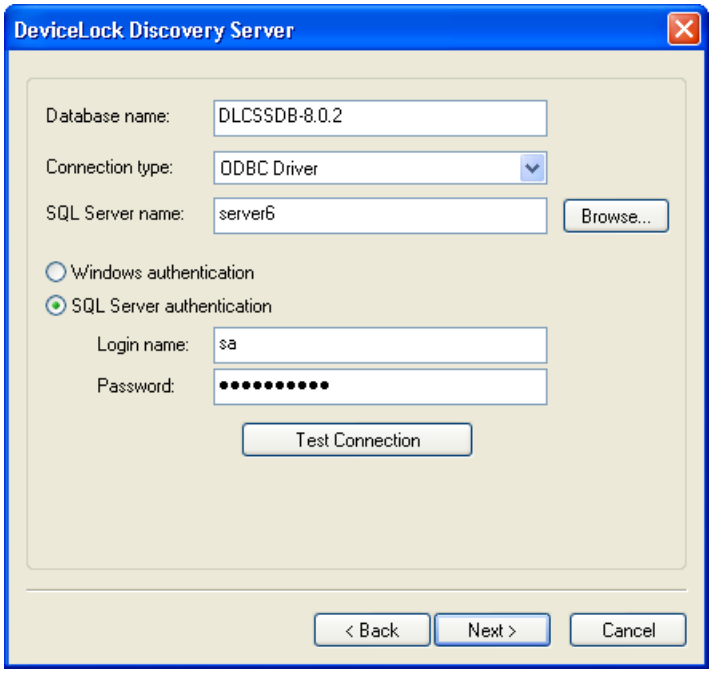
The trial period for DeviceLock Content Security Server is 30 days.

Click **Next** to apply the loaded licenses, and proceed to the next page of the configuration wizard.

Database Connection
During this step, you will need to configure the connection to a SQL Server database.

Note: This step is only needed if you require the Discovery functionality. If you are not interested in the Discovery, you may click **Cancel** to skip this step. If this is the case, the Setup wizard will close, while all previously configured settings will be correctly applied and saved.

On this page, you can configure database parameters.



Database name

You must specify the name of the database in SQL Server that will be used to store the DeviceLock Discovery Server data. The default name suggested by the wizard is **DLCSSDB**.

Note: You should not create a database with the specified name manually because the configuration wizard creates the database automatically or uses the existing one.

Connection type

There are two ways to define a connection to SQL Server:

1. **ODBC Driver** – you enter the name of SQL Server in **SQL Server name** and select the authentication mode (Windows or SQL Server).

   The **SQL Server name** parameter must contain not just the name of the computer where SQL Server is running but the name of SQL Server itself. Usually the SQL Server name consists of two parts: the computer name and the instance name divided by a backslash (e.g. computer\instance). Sometimes the instance name is empty (default) and you can use the computer name as an SQL Server name. To retrieve SQL Server names available in your local network, press the **Browse** button. (You should have access to the remote registry of the SQL Server machine to retrieve the instance name.)

   If the **SQL Server name** parameter is empty, it means that SQL Server is running on the same computer as DeviceLock Content Security Server and has an empty (default) instance name.

To establish a connection to SQL Server, you must also configure authentication parameters.

Select the **Windows authentication** option to authenticate on SQL Server under the account used to run DeviceLock Content Security Server's service.

If the service is running under the SYSTEM user and SQL Server is located on the remote computer, service will not be able to connect to SQL Server since the SYSTEM user doesn't have a right to access the network. For more information on how to run DeviceLock Content Security Server on behalf of the user, please read the description of the Log on as parameter.

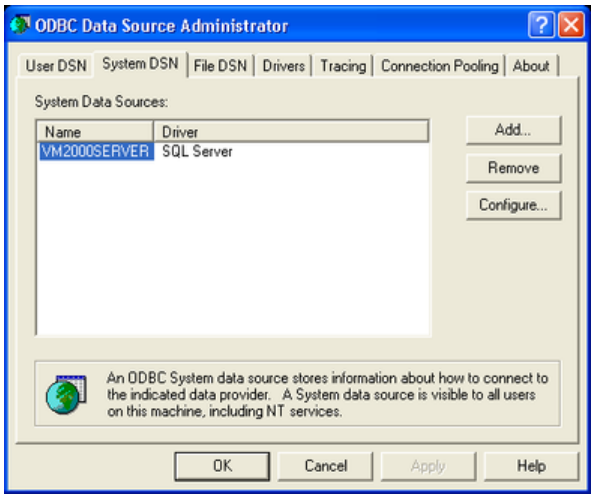
Select the **SQL Server authentication** option to allow SQL Server to perform the authentication itself by checking the login and password previously defined. Before selecting the **SQL Server authentication** option, make sure that your SQL Server was configured to use mixed-mode authentication.

Enter the SQL user name (login) in **Login name** and its password in **Password**.

Note: Windows Authentication is much more secure than SQL Server Authentication. When possible, you should use Windows Authentication.

2. **System Data Source** – you select the predefined system data source from the **Data Source Name** list.

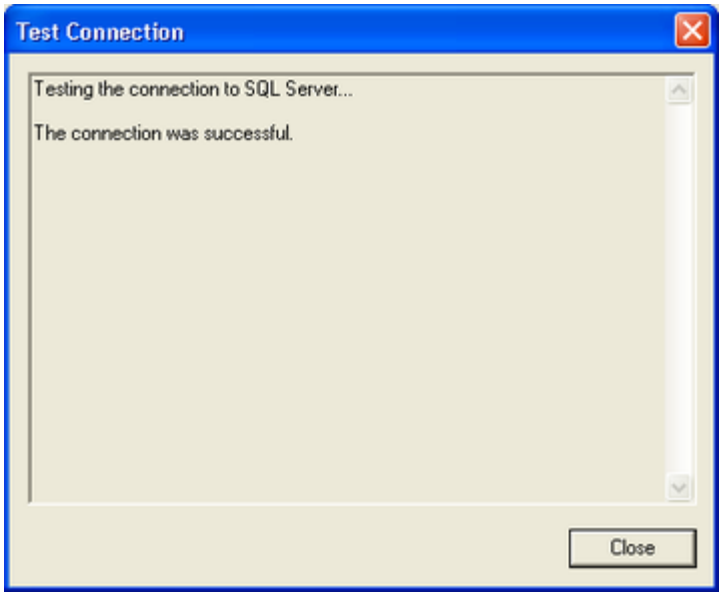
   To define data sources, use the **Data Sources (ODBC**) applet from **Control Panel** -> **Administrative Tools**.



   If, in the data source configuration, SQL Server Authentication was chosen, then you also need to specify the SQL user name (login) in **Login name** and its password in **Password**. If Windows Authentication was selected, then you should leave these fields blank.

   To refresh the **Data Source Name** list, press the **Refresh** button.

When connection to SQL Server is defined you may want to test it. Press the **Test Connection** button to make sure that all the parameters were specified correctly.



Please note that it only checks connectivity and your access rights to SQL Server. If there are problems with the database or your access rights to this database, you don't see those problems in the **Test Connection** dialog box.

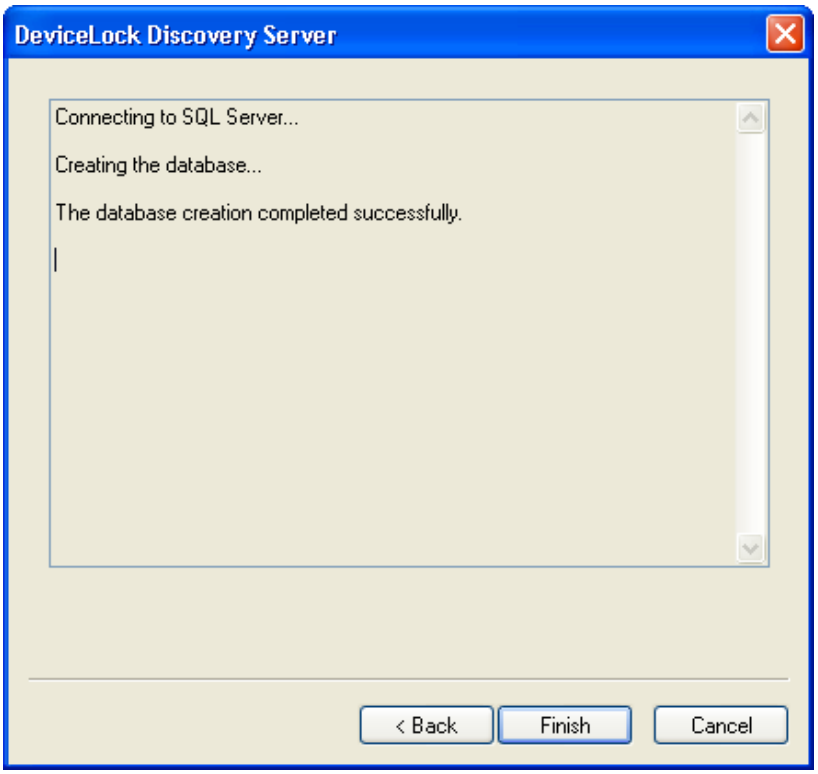
If some connection parameters were specified incorrectly, you may see one of these errors:

- **SQL Server does not exist or access denied** – you've specified an incorrect name of SQL Server in the **SQL Server name** parameter or the remote SQL Server's computer is not accessible. It is possible that you've specified the name of the computer where SQL Server is running but this SQL Server also has an instance name which should be specified as well (e.g. computer\instance).
- **Login failed for user 'COMPUTER_NAME$'** – you've selected Windows Authentication but the user account used to run the DeviceLock Content Security Server service can't get access to the computer with SQL Server. It may happen when the service starts either under the SYSTEM user or on behalf of a user that doesn't have local administrative privileges on the remote SQL Server's computer.
- **Login failed for user 'user_name'** – you've selected SQL Server Authentication and either specified an incorrect SQL user name (login) or the wrong password for it. Please note that SQL users are different from Windows users and you can't use the regular Windows account in the **Login name** parameter. SQL users exist only in SQL Server and to manage them you should use SQL Server management consoles (such as Microsoft SQL Server Management Studio).
- **Login failed for user 'user_name'. The user is not associated with a trusted SQL Server connection** – you've selected SQL Server Authentication but your SQL Server doesn't support this mode. You should

either use Windows Authentication or allow your SQL Server to work in the mixed mode (SQL Server and Windows Authentication mode).

- **Login failed for user ''. The user is not associated with a trusted SQL Server connection** – the data source you've specified in **Data Source Name** was configured to use the SQL Server Authentication mode but the **Login name** parameter is empty.
- **Data source name not found and no default driver specified** – you've selected **System Data Source** from the **Connection type** list and specified either an empty or non-existent name in **Data Source Name**.

Press the **Next** button to apply changes and proceed to the last page.



It takes some time to create the database specified in **Database name** if it does not exist on this SQL Server yet. If the database already exists and it has the proper format (i.e. was created by DeviceLock Discovery Server) then DeviceLock Discovery Server keeps all existing data and uses this database.

Note: If necessary, DeviceLock Discovery Server automatically updates the database to the latest version.

If some parameters on the previous wizard's page were specified incorrectly, you may see one of these errors:

- **CREATE DATABASE permission denied in database 'name'** – the user's account (login) used to connect to SQL Server doesn't have enough privileges to create the database. The login should have at least the dbcreator Server role (see **Server Roles** in **Login Properties** of Microsoft SQL Server Management Studio).
- **The server principal "user_name" is not able to access the database "name" under the current security context** – the user's account (login) used to connect to SQL Server doesn't have access to the existing database. The login should be mapped to this database (see **User Mapping** in **Login Properties** of Microsoft SQL Server Management Studio).
- **SELECT permission denied on object 'name', database 'name', schema 'name'** – the user's account (login) used to connect to SQL Server doesn't have read/write access to the existing database. The login should have at least db_datareader and db_datawriter Database roles (see **User Mapping** in **Login Properties** of Microsoft SQL Server Management Studio).
- **Invalid object name 'name'** – the database specified in the **Database name** parameter already exists in this SQL Server but has an incorrect format. It happens when you are trying to use the database that was not created by DeviceLock Discovery Server or if the database was corrupted.
- **DeviceLock Database has an unsupported format** – the database specified in the **Database name** parameter already exists but is outdated. This existing database has an unsupported format so it can't be automatically upgraded to the new format. You should either use another database or create a new one.
- **DeviceLock Database has a format that is not supported by the current server version** – the database specified in the **Database name** parameter already exists but it was created by the more recent version of DeviceLock Discovery Server. You should either use the latest version of DeviceLock Discovery Server or use another database (or create a new one).

Also, some of the SQL Server connection errors described above may be displayed here as well.

Use the **Back** button to return to the previous page of the wizard and make necessary changes.

If there are no errors, press the **Finish** button to close the wizard and continue the installation process.

Next, on the **Installation Wizard Completed** page, click **Finish** to complete the installation. On this page, you will have the option to go to the DeviceLock home page. This option is selected by default.

Note: To uninstall DeviceLock Content Security Server, do one of the following:

Use **Add or Remove Programs** in Control Panel to remove **DeviceLock Content Security Server**.
- OR -
Click **Start**, point to **All Programs**, point to **DeviceLock**, and then click **Remove DeviceLock Content Security Server**.

DeviceLock Certificates

Overview

DeviceLock Certificate is a cryptographic certificate that consists of two keys (the key pair): private and public:

- The private key must be stored on the administrator's computer and only the administrator must be able to access it. Also, the private key may be installed on DeviceLock Enterprise Server and DeviceLock Content Security Server.

  Note: Make sure that non-administrative users can't get access to the private key.

- The public key is installed on every computer where DeviceLock Service is running. If the public key has not been preinstalled on the user's computer, there is no way to use the Temporary White List function or DeviceLock Certificate authentication on DeviceLock Enterprise Server.

Generating DeviceLock Certificates

DeviceLock's Certificate Generation Tool allows you to generate DeviceLock Certificates.

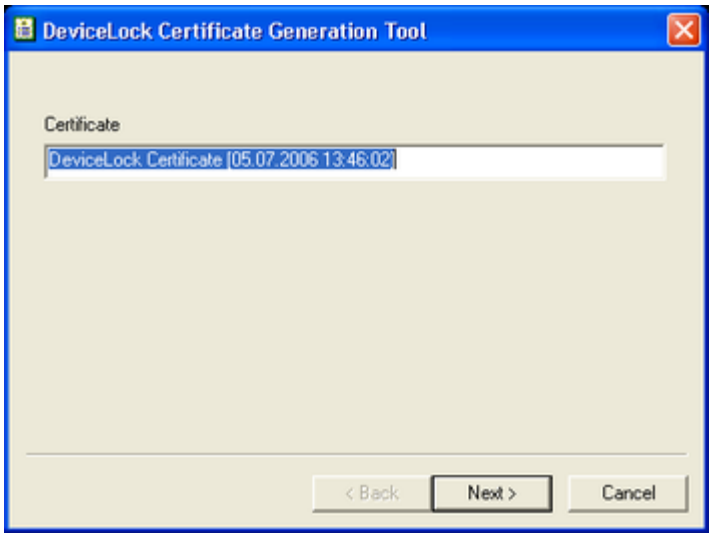
We recommend that you generate only one DeviceLock Certificate and deploy its public key to all user computers. It is necessary to generate and install a new certificate only if the private key was either compromised (e.g. stolen) or lost.

To run the Certificate Generation Tool, select the **Certificate Generation Tool** item from the **File** menu in DeviceLock Enterprise Manager. To run the Certificate Generation Tool from DeviceLock Management Console (the MMC snap-in) and DeviceLock Group Policy Manager, use the context menu available by a right mouse click.

The Certificate Generation Tool will run automatically when DeviceLock management consoles are installed on an administrator's computer that has no DeviceLock Certificate.

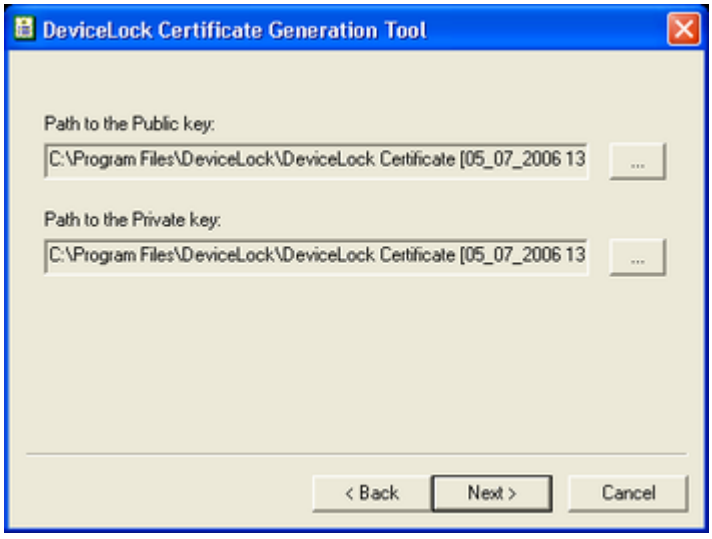
There are two simple steps to generate the key pair:

1. Define the name of the DeviceLock Certificate.



The Certificate Generation Tool auto-generates a name based on the current date and time, but you can type any other name.

2. Define the path and file names for private and public keys.



As soon as the DeviceLock Certificate is generated, you can start deploying the public key to users' computers.

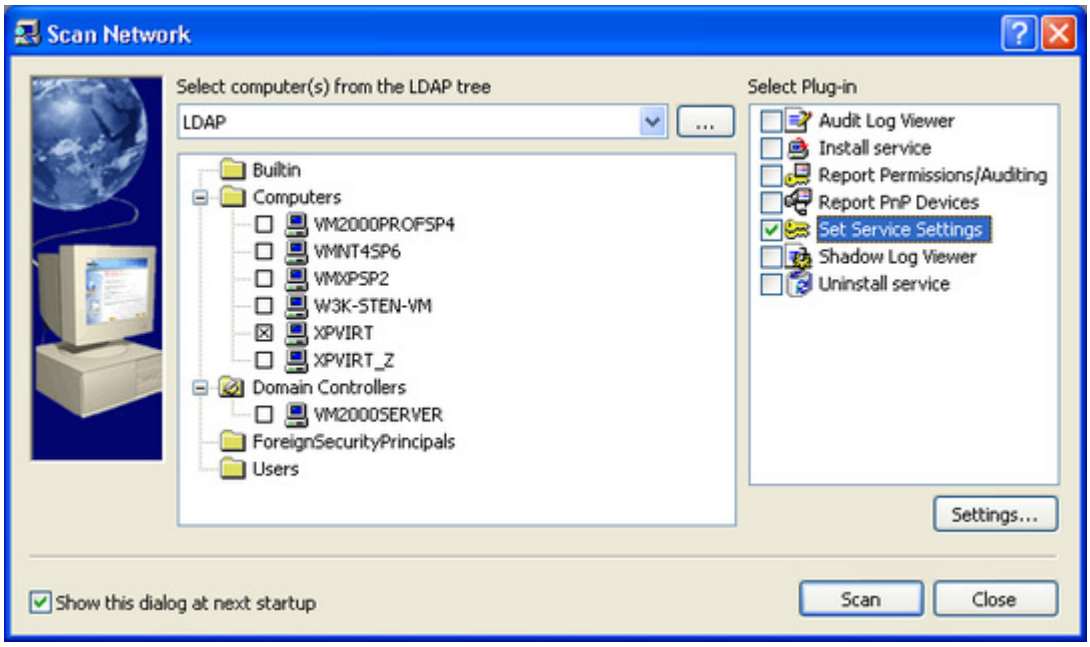
Note: A newly generated DeviceLock Certificate does not automatically install on computers from the Certificate Generation Tool. You must deploy it manually from a DeviceLock management console.

Installing/Removing DeviceLock Certificate

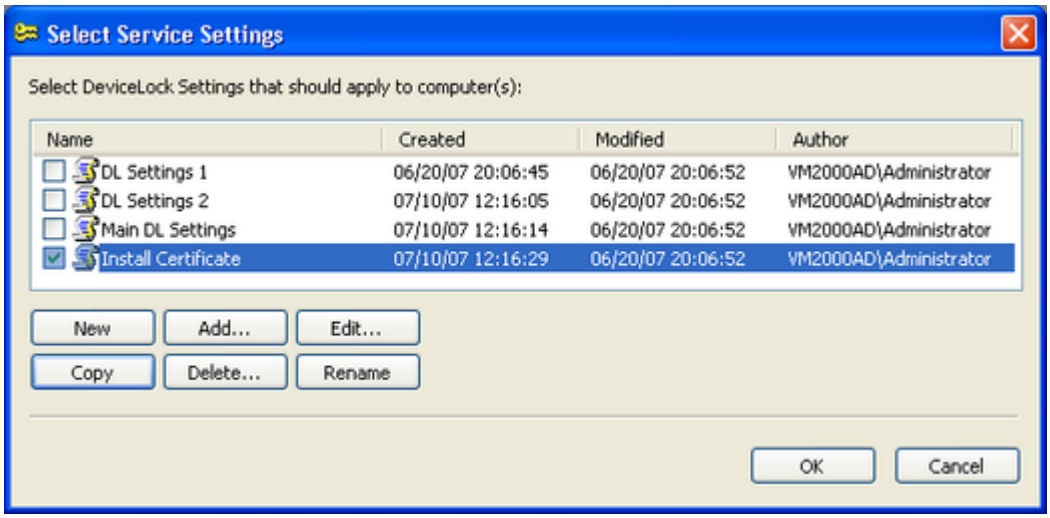
To install/remove the public key on/from user computers running DeviceLock Services, you can use any DeviceLock management console:

- DeviceLock Enterprise Manager

  On the **Scan Network** dialog box, select the computers targeted for installation/removal of the public key and select the **Set Service Settings** plug-in.



  Press the **Settings** button or double-click on the plug-in's record to open the configuration dialog box.

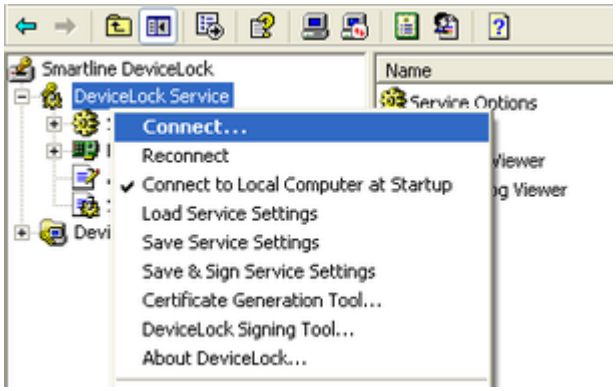


Create the new XML file or use the existing one to define the policy needed to install/remove the certificate. Highlight the file in the list and then press the **Edit** button to modify the policy as described in the next section (below). When finished modifying the policy, select its file by enabling the checkmark next to the file's name in the list.

Press the **OK** button to close the configuration dialog box and then press the **Scan** button on the **Scan Network** dialog box to start the DeviceLock Certificate installation/removal process.

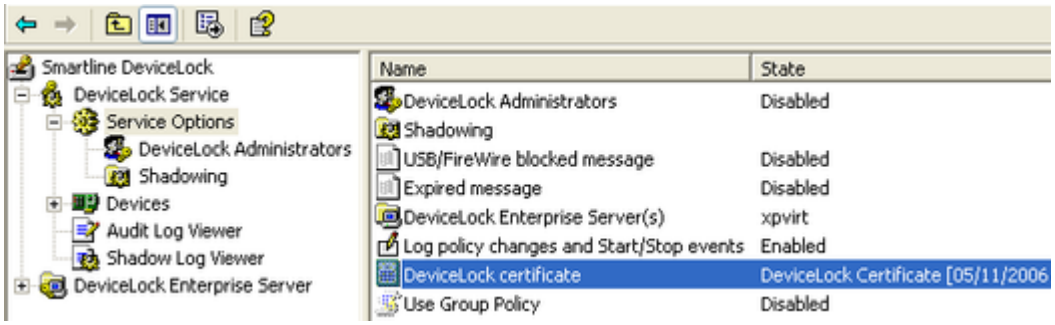
- DeviceLock Management Console, DeviceLock Group Policy Manager and DeviceLock Service Settings Editor

  If you are using DeviceLock Management Console (the MMC snap-in), first you need to connect it to the computer running DeviceLock Service. Use the context menu available by a right mouse click.



When DeviceLock Group Policy Manager is used, you don't need to connect to any computer since it connects to the Group Policy Object. Also, you don't need to connect to the computer when modifying the policy in the XML file using DeviceLock Service Settings Editor.

Activate the **Service Options** item.



Double-click the **DeviceLock certificate** parameter to open the configuration dialog box.

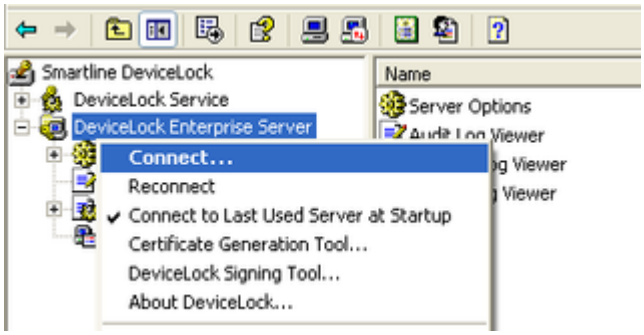
Specify the path to the public key in the **Certificate Name** parameter if you want to install the certificate. You can use the **...** button to select the file with a public key.

To remove the public key, use the **Remove** button.

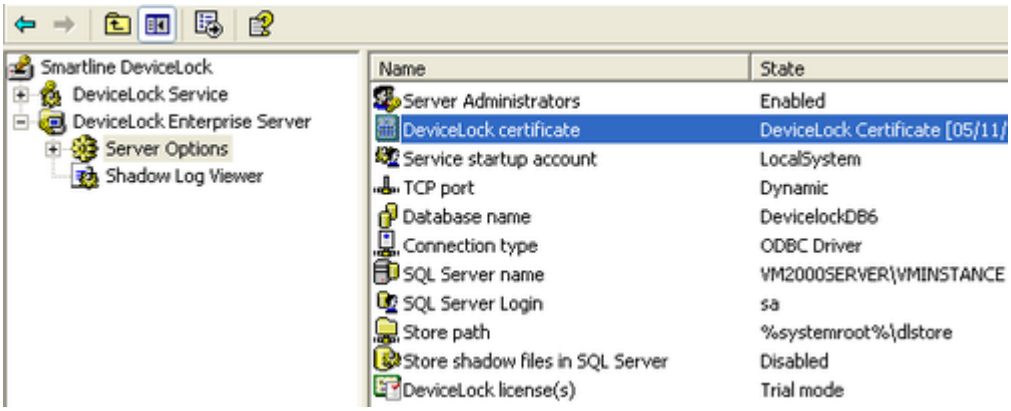
Press the **OK** button to close the configuration dialog box and apply changes.

To install/remove the private key on/from DeviceLock Enterprise Server and DeviceLock Content Security Server, you can use DeviceLock Management Console (the MMC snap-in).

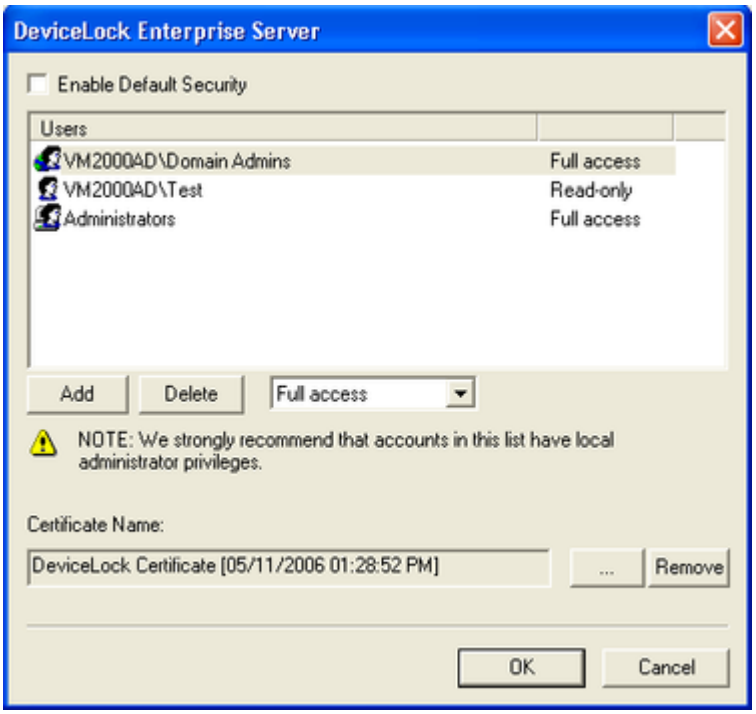
You need to connect DeviceLock Management Console to the computer running DeviceLock Enterprise Server or DeviceLock Content Security Server. Use the context menu available by a right mouse click.



Activate the **Server Options** item.



Double-click the **DeviceLock certificate** parameter to open the configuration dialog box.



Specify the path to the private key in the **Certificate Name** parameter if you want to install the certificate. You can use the **...** button to select the file with a private key.

To remove the private key, use the **Remove** button.

Press the **OK** button to close the configuration dialog box and apply changes.

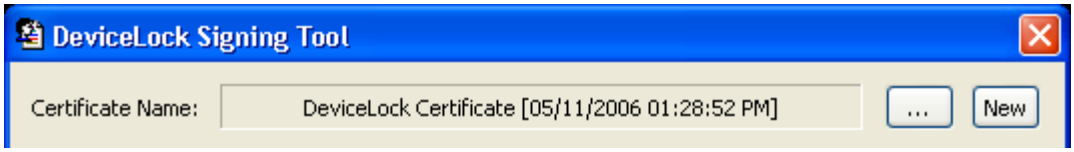
For more information regarding installing the private key on DeviceLock Enterprise Server and DeviceLock Content Security Server, please read Installing DeviceLock Enterprise Server and Installing DeviceLock Content Security Server sections of this manual.

DeviceLock Signing Tool

Overview

The DeviceLock Signing Tool is used to grant users temporary access to requested devices and sign XML files containing DeviceLock Service settings exported from DeviceLock Management Console or DeviceLock Group Policy Manager.

To run the DeviceLock Signing Tool, select **DeviceLock Signing Tool** from the **File** menu in DeviceLock Enterprise Manager or from the context menu in DeviceLock Management Console (the MMC snap-in), DeviceLock Group Policy Manager or DeviceLock Service Settings Editor.



First of all you should load the corresponding DeviceLock Certificate (the private key).

The DeviceLock Signing Tool must use the private key that belongs to the same certificate as the public key installed on the user's computer.

By default, the DeviceLock Signing Tool automatically loads the last certificate used. You can load another certificate by pressing the **...** button and selecting a file with the private key.

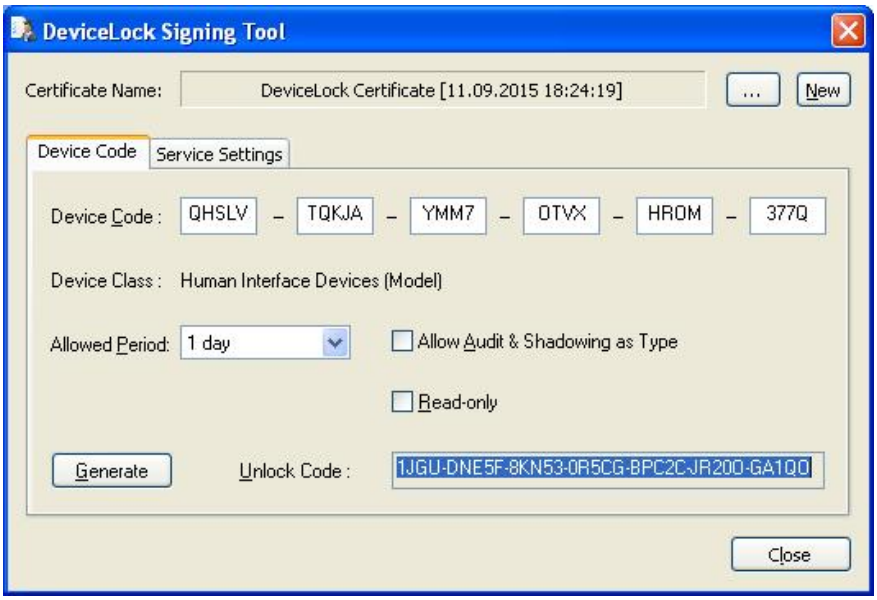
To generate the new certificate you can run the Certificate Generation Tool directly from the DeviceLock Signing Tool. To do so, you should press the **New** button. However, please keep in mind that if you generate a new certificate and intend to use its new private key in the DeviceLock Signing Tool, you must also deploy the corresponding public key on the user's computer.

Then, decide what action you want to perform: generate an Unlock Code or sign an XML file containing DeviceLock Service settings.

Device Code

To grant the user temporary access to a requested device you should generate an Unlock Code upon receiving the Device Code from this user.

For more information on using temporary white list, please read the Temporary White List section of this manual.



There are four simple steps to generating an Unlock Code for the user:

1. Load the corresponding DeviceLock Certificate (see above).
2. Enter the Device Code, the user provides to you.

   As soon as the correct Device Code is entered, you can see the class of the device the user wants access to in the **Device Class** field. The device class information helps you to control what kind of device the user is going to use. If, for example, a user tells the administrator that he/she is going to use a USB scanner but actually is trying to obtain access to a USB flash drive, the administrator would recognize the discrepancy.

   There is also a field (in round brackets) showing whether the requested device can be authorized as a unique device (**Unique**) or can be authorized only as a model (**Model**), i.e. whether or not it has a serial number. If you authorize the device as a model, then the user is granted access to all devices of this model. For more information on this, please read the USB Devices White List section of this manual.

3. Select the period when the requested device will be allowed. In **Allowed Period**, you can select several predefined periods: 5, 15, 30, 60 minutes, 5 hours, 1 or 2 days, 1 or 2 weeks, 1 month, until the device is unplugged or until the user is logged off.

   When you select a fixed time period (e.g. 10 minutes), the user is granted access to the requested device for only this period. As soon as the allowed time expires, access to the device is denied again. It doesn't matter what the user is doing with this device – even if he/she is still copying files onto the USB disk or printing a document on the USB printer, all operations will be aborted.

   To allow the user to use a requested device without any time limitations, select until unplug in **Allowed Period**. The user is then granted access to the device while it is plugged into the port. As soon as the user unplugs this device, access to it is denied again.

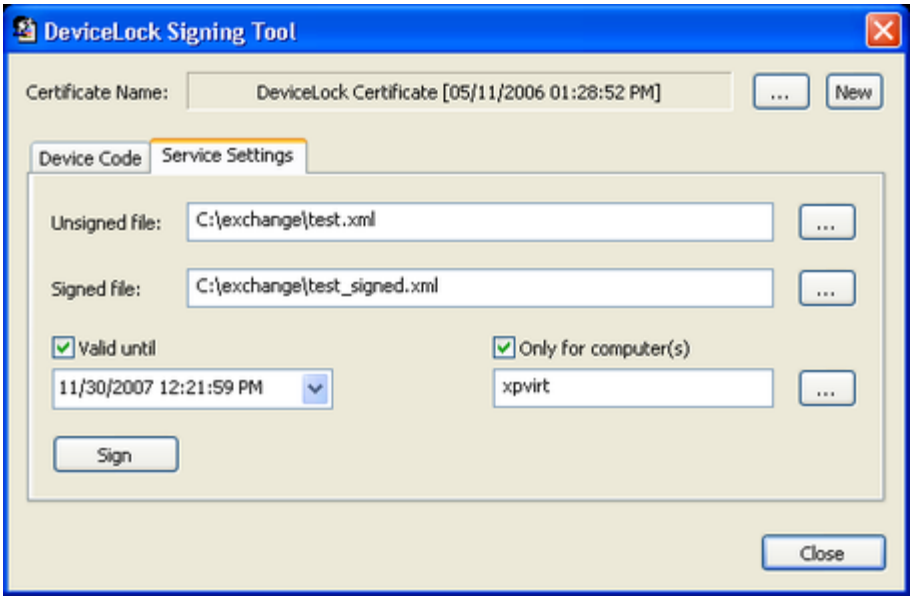
4. Press the **Generate** button to create an Unlock Code. Provide this code to the user over the phone or in any other suitable way.

   The process of generating an Unlock Code can be a time-consuming operation. It depends on your computer's processing speed and could take as long as several seconds.

Service Settings

To avoid unauthorized modification you can sign an XML file containing DeviceLock Service settings exported from DeviceLock Management Console or DeviceLock Group Policy Manager or created using DeviceLock Service Settings Editor.

Later this file can be sent to users whose computers are not online and thus out-of-reach via management consoles.



There are six simple steps to signing an XML file:

1. Load the corresponding DeviceLock Certificate (see above)
2. Load the file with DeviceLock Service settings you need to sign.

   The full path to this file must be specified in the **Unsigned file** field. You can use the **...** button to select the file.

   *The XML file with DeviceLock Service settings can be created using **Save Service Settings** from the context menu in DeviceLock Management Console, DeviceLock Group Policy Manager or DeviceLock Service Settings Editor.*
3. In the **Signed file** field, specify the resultant file. You can use the **...** button to select the folder where this file will be created.
4. Decide whether the resultant file should contain expiration information or not.

If you want to allow users to import settings from this file without any time limitations, disable the **Valid until** flag.

If you enable the **Valid until** flag and specify the date/time, then the expiration information writes to the resultant file and users can import settings from this file only before the specified date/time.

Please note that this parameter affects only users that are trying to import DeviceLock Service settings via the DeviceLock applet from the Windows Control Panel. When an XML file with settings is loaded using **Load Service Settings** from the context menu in DeviceLock Management Console or DeviceLock Group Policy Manager, the expiration information (if any) is ignored.

5. Decide whether the resultant file can be used only on specific computers or not.

   If you want to allow users to import settings from this file on any computers, disable the **Only for computer(s)** flag.

   If you enable the **Only for computer(s)** flag and specify the computer name then users will be able to import settings from this file only on this specified computer. Using the semicolon (;) as a separator, you can specify several computer names such that the resultant file can be used on any of these computers.

   Note: You can't use the computer's IP address in this parameter. You must specify the computer name exactly as it is displayed in the System applet from the Windows Control Panel.

   On Mac computers the name reported by the **hostname** command must be used. The same name is available in **System Preferences -> Sharing**.

   You can also load a predefined list of computers from the external text file. To open an external file, press the **...** button. This text file must contain each computer's name on separate lines.

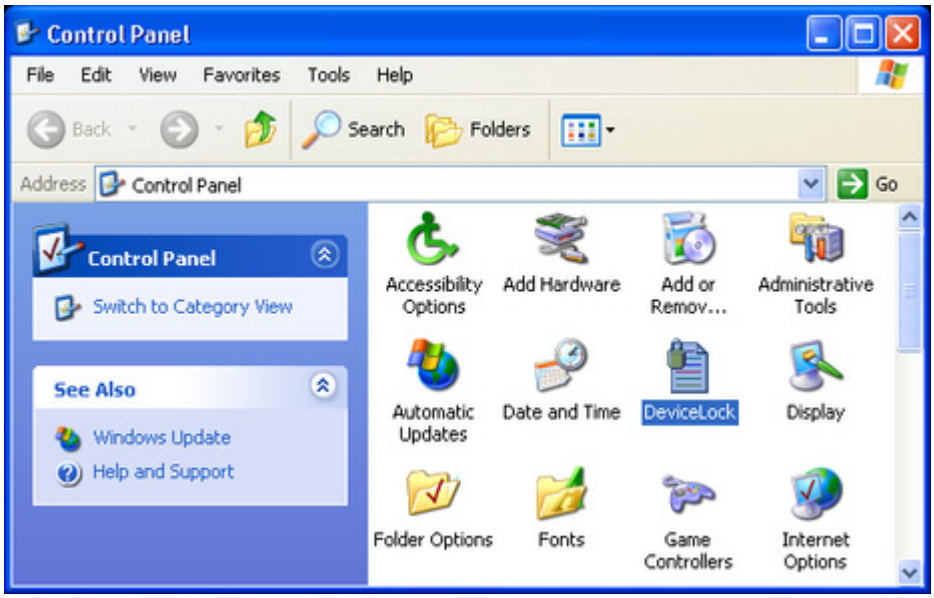
   Please note that this parameter affects only users that are trying to import DeviceLock Service settings via the **DeviceLock** applet from the Windows Control Panel. When an XML file with settings is loaded using **Load Service Settings** from the context menu in DeviceLock Management Console or DeviceLock Group Policy Manager, the computer's name information is ignored.

6. Press the **Sign** button to create a signed file with DeviceLock Service settings. Provide this file to the user in any suitable way.

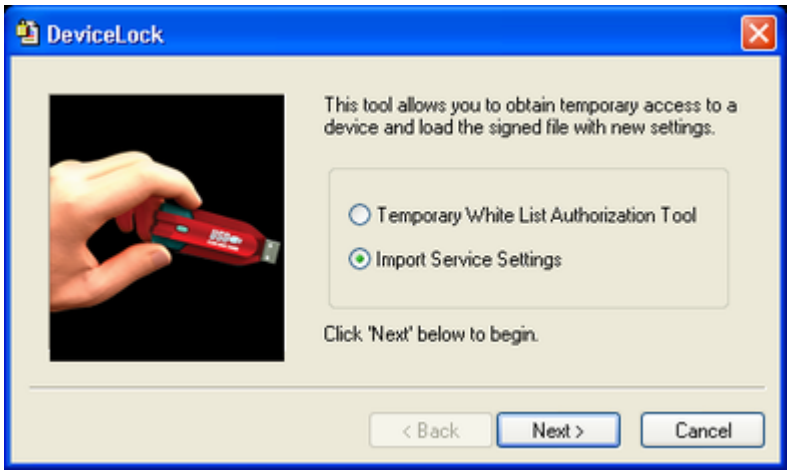
   The process of file signing can be a time-consuming operation. It depends on your computer's processing speed and could take as long as several seconds.

Loading signed settings file on Windows

When the user wants to apply DeviceLock Service settings from this signed file, he/she should run the **DeviceLock** applet from the Control Panel and select the **Import Service Settings** option.

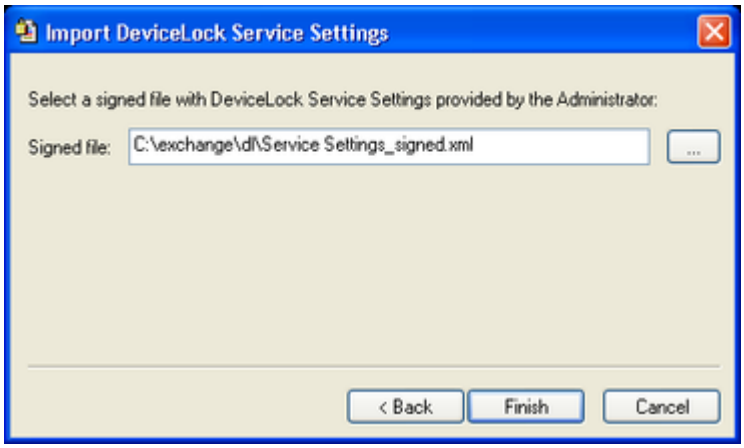


Note: On Windows XP and later, the user must switch the Control Panel to Classic View in order to view all available applets.


DeviceLock
This tool allows you to obtain temporary access to a device and load the signed file with new settings.
Temporary White List Authorization Tool
Import Service Settings
Click 'Next' below to begin.
< Back
Next >
Cancel

There are two simple steps for the user to import DeviceLock Service settings from the signed file:

1. In the **Signed file** field, specify the full path to this signed file. Use the **...** button to select the file.



2. Press the **Finish** button. If the digital signature in the file is valid, then the new settings will be applied to DeviceLock Service immediately.

The user can also load the signed file with DeviceLock Service settings using the command line:

DLTempAccess.cpl -s *<path to signed file>*

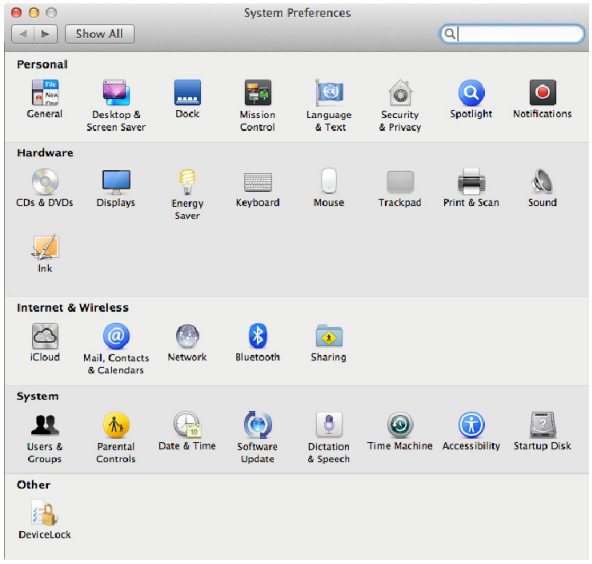
where *<path to signed file>* is the path to the signed file with DeviceLock Service settings. For example:

DLTempAccess.cpl -s "C:\Program Files\DeviceLock\settings_signed.dls"

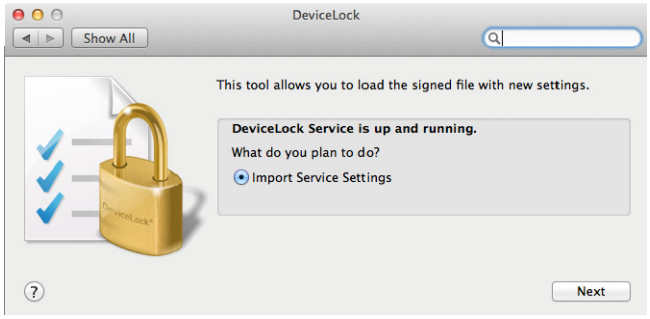
All successful attempts to load settings are logged, if logging of changes is enabled in the Service Options.

Loading signed settings file on Mac

DeviceLock Service for Mac installs its Preference Pane into System Preferences at **System Preferences -> DeviceLock**.

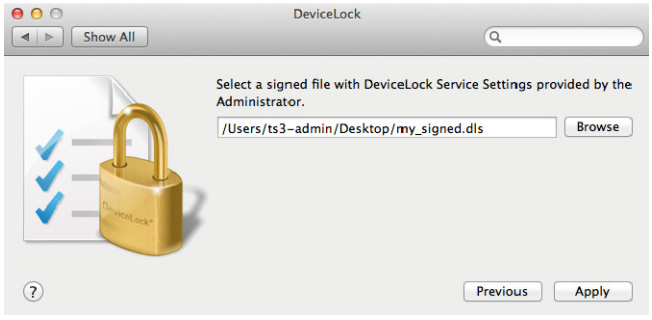


When the user wants to apply DeviceLock Service settings from this signed file, he/she should run the **DeviceLock** pane from System Preferences and select the **Import Service Settings** option.

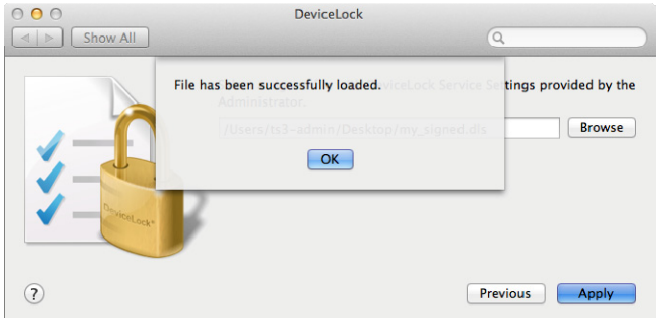

DeviceLock
Show All
This tool allows you to load the signed file with new settings.
DeviceLock Service is up and running.
What do you plan to do?
Import Service Settings
Next

There are two simple steps for the user to import DeviceLock Service settings from the signed file:

1. In the **Signed file** field, specify the full path to this signed file. Use the **Browse** button to select the file.



2. Press the **Apply** button. If the digital signature in the file is valid, then the new settings will be applied to DeviceLock Service for Mac immediately.



The user can also load the signed file with DeviceLock Service settings using the command line:

/Library/DeviceLockAgent/Utilities/DLAgentControl importdls *<path to signed file>*

where *<path to signed file>* is the full relative path to the signed file with DeviceLock Service settings. For example:

/Library/DeviceLockAgent/Utilities/DLAgentControl importdls /home/user/Desktop/settings_signed.dls

Note: If DeviceLock Administrators are configured, a non-administrative user will not be able to access the /Library/DeviceLockAgent/Utilities folder even in read-only mode. The administrator must copy DLAgentControl to a different location. Alternatively, the application is available in the Utilities folder on the installation .dmg image.

All successful attempts to load settings are logged, if logging of changes is enabled in the Service Options.

DeviceLock Management Console

Overview

DeviceLock Management Console is a snap-in for Microsoft Management Console (MMC).

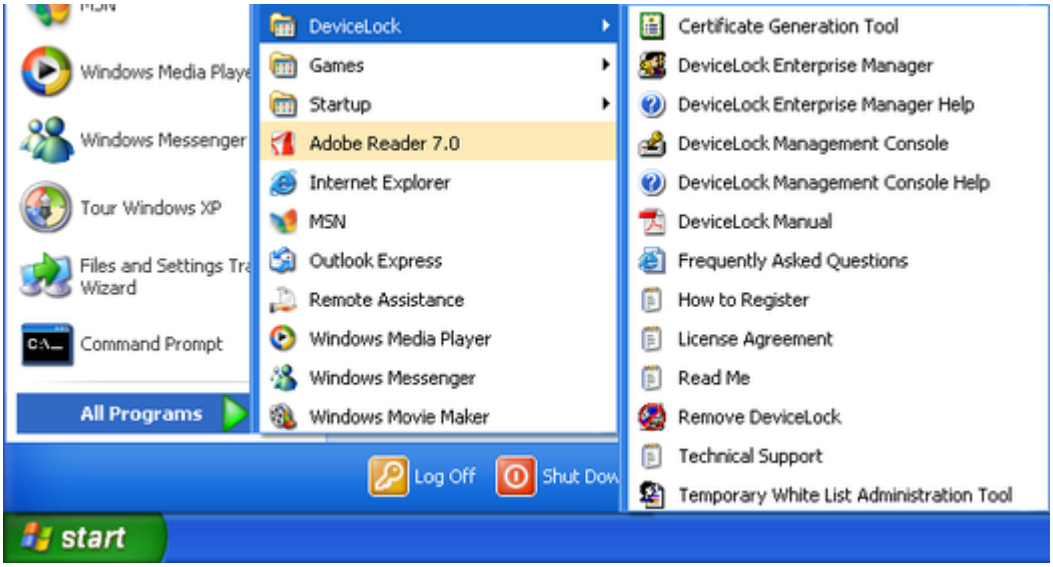
Using DeviceLock Management Console, you can view and change permissions and audit rules, install and update DeviceLock Service as well as view audit records for individual computers.

Also, DeviceLock Management Console is used for viewing logs stored on DeviceLock Enterprise Server, running search queries on DeviceLock Content Security Server and for managing these servers.

DeviceLock Management Console should be used on the computer from which the administrator is managing DeviceLock Services, DeviceLock Enterprise Servers and DeviceLock Content Security Servers on the network.

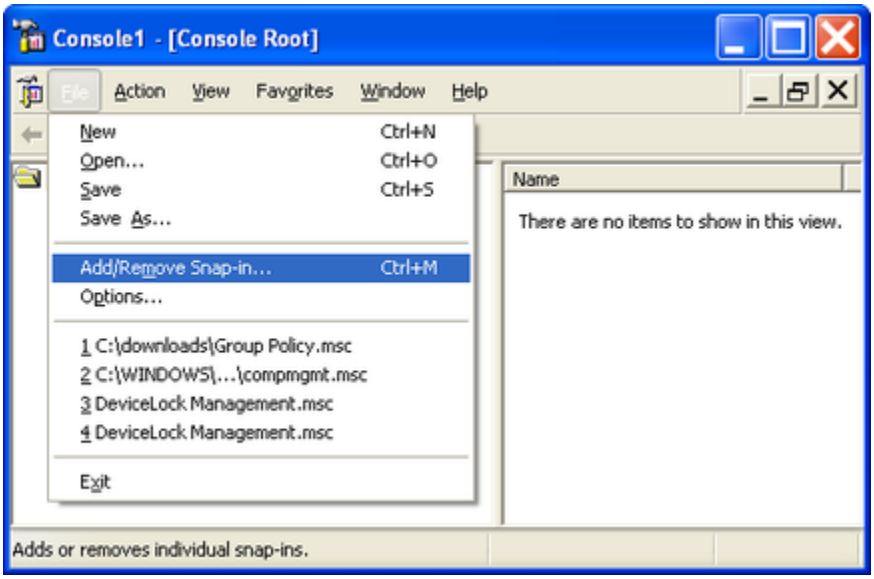
For information on how to install DeviceLock Management Console, please read the Installing Management Consoles section of this manual.

To run DeviceLock Management Console, select the appropriate shortcut from the **Programs** menu available by clicking the Windows **Start** button.

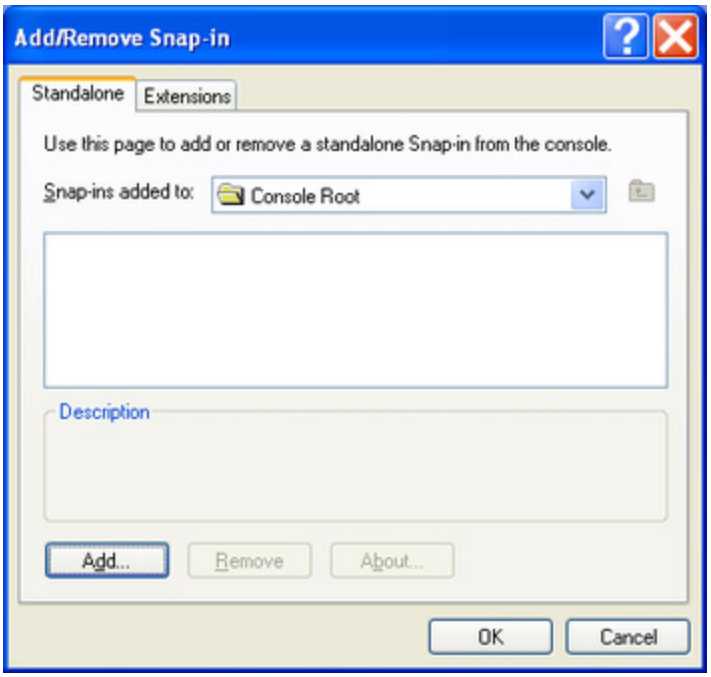


Alternatively, you can start MMC and add the DeviceLock Management Console snap-in manually:

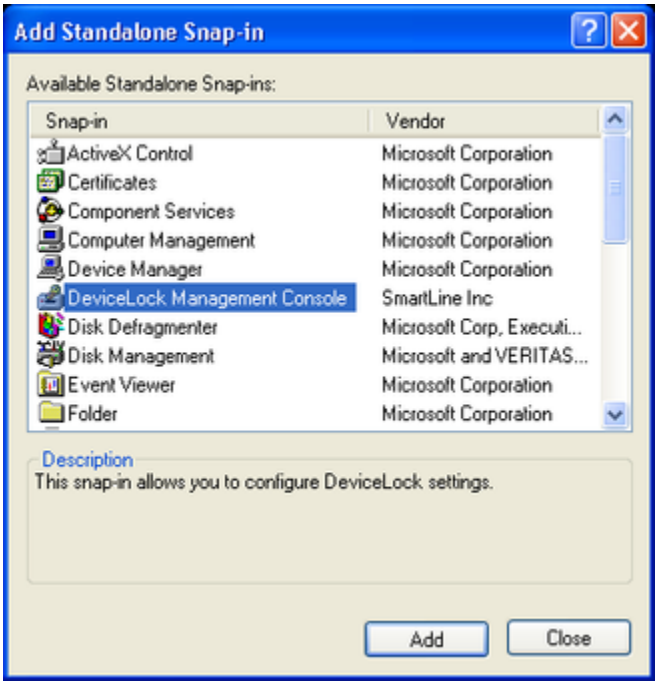
1. Run **mmc** from the command line or use the **Run** menu to execute this command.
2. Open the **File** menu, and then click **Add/Remove snap-in**.



3. Click the **Standalone** tab, and then click **Add**.

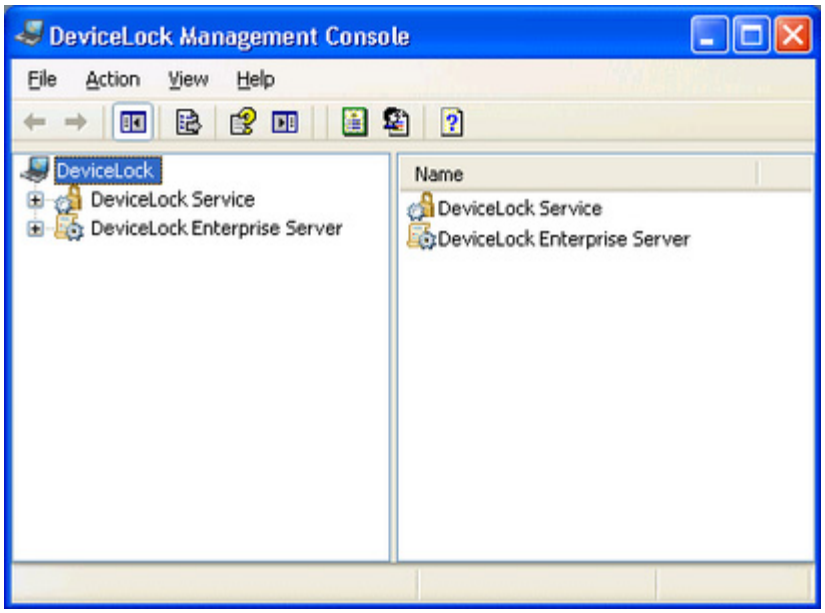


4. Select **DeviceLock Management Console** from the list, then click **Add**.



Interface

DeviceLock Management Console has a user-friendly, easy-to-use standard interface provided by Microsoft Management Console (MMC). At any time, you can press the F1 key to get context-specific help.



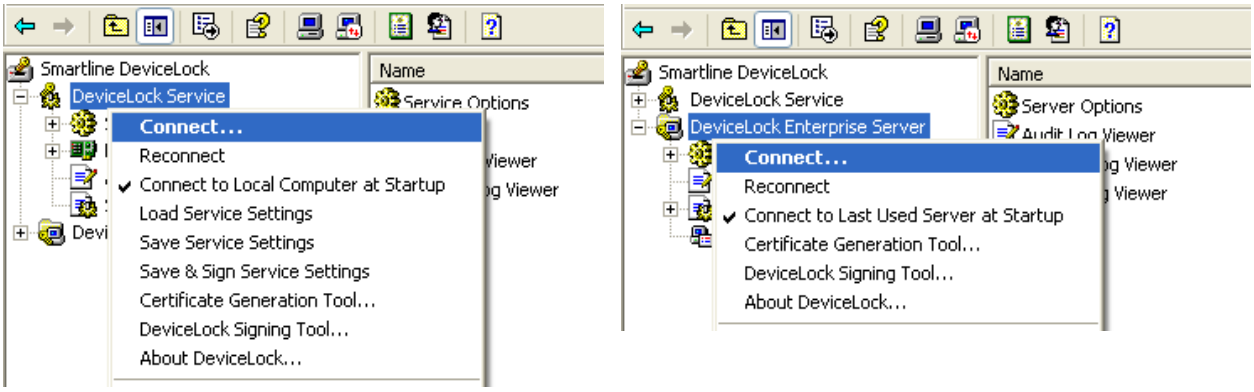
DeviceLock Management Console consists of a window divided into two panes. The left pane contains the console tree; the right pane contains details. When you select an item in the console tree, information about that item is displayed in the details pane.

There are three independent parts in DeviceLock Management Console:

1. **DeviceLock Service** – allows you to connect to and manage DeviceLock Services running on remote and local computers.
2. **DeviceLock Enterprise Server** – allows you to connect to and manage DeviceLock Enterprise Servers running on remote and local computers.
3. **DeviceLock Content Security Server** – allows you to connect to and manage DeviceLock Content Security Servers running on remote and local computers.

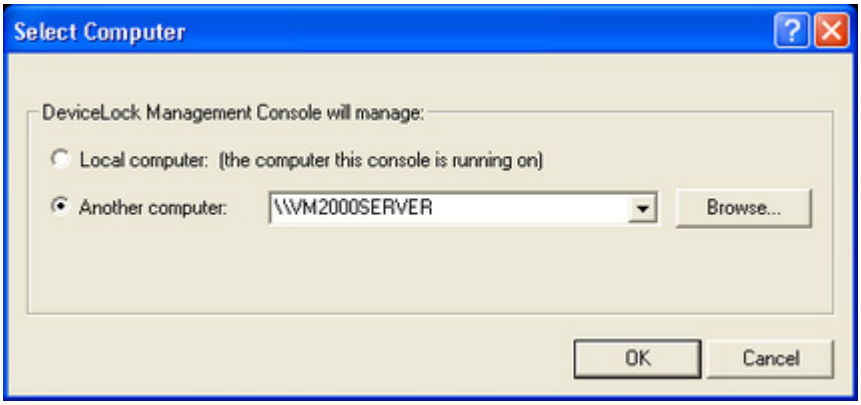
Connecting to Computers

First of all, you should connect to the computer where DeviceLock Service, or DeviceLock Enterprise Server, or DeviceLock Content Security Server is running. Use the context menu **Connect** item or the appropriate button on the toolbar.



You can simultaneously connect to DeviceLock Service, DeviceLock Enterprise Server and DeviceLock Content Security Server even if they are running on different computers.

Specify the remote computer name or IP address you want to connect to in the **Another computer** parameter. To browse for available computers in your network, use the **Browse** button.



To connect DeviceLock Management Console to the computer where DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server was configured using a

fixed port, you should specify this port in square brackets next to the computer name, e.g. *\\computer_name[port number]*.

To connect to the local computer, use the **Local computer** option.

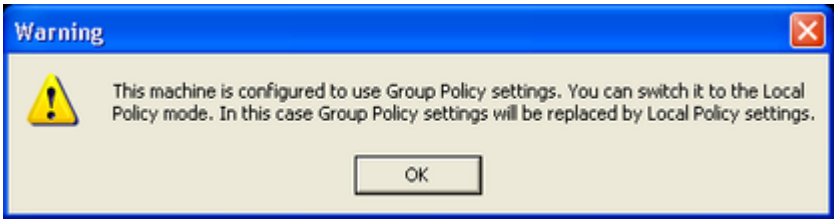
Press the **OK** button to connect to the selected computer.

Note: Make sure that the remote computer you've selected to connect to is accessible from the computer where DeviceLock Management Console is running. The remote computer must work under a DeviceLock-compatible OS (Windows NT 4.0 SP6 and later). It must have a functioning TCP/IP protocol. In case a firewall (including built-in Windows Firewall) is installed on the remote computer, it must be properly configured to allow connection with DeviceLock Service, DeviceLock Enterprise Server and/or DeviceLock Content Security Server.

DeviceLock Service (as well as DeviceLock Enterprise Server and DeviceLock Content Security) automatically adds itself to the exception list of Windows Firewall.

When you're trying to connect to DeviceLock Service on a computer where it is not installed or is outdated, DeviceLock Management Console suggests that you install or update the service. For more information regarding the remote service deployment, please read the Remote Installation via DeviceLock Management Console section of this manual.

You receive the warning message when you connect to DeviceLock Service configured to work in the Group Policy mode.


Warning
This machine is configured to use Group Policy settings. You can switch it to the Local Policy mode. In this case Group Policy settings will be replaced by Local Policy settings.
OK

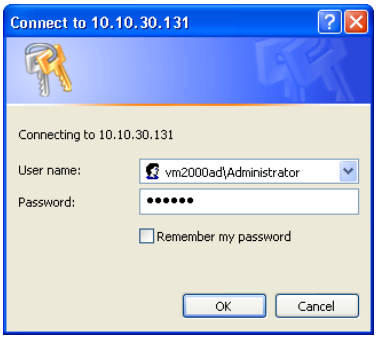
If you change some parameter using DeviceLock Management Console, it will revert to its original state (defined in GPO) on the next Group Policy update. For more information, please read the Service Options section of this manual.

If you're trying to connect to DeviceLock Enterprise Server or DeviceLock Content Security Server on a computer where it is not installed or stopped, you receive a connection error.

DeviceLock Enterprise Server and DeviceLock Content Security Server must be installed and started before DeviceLock Management Console can connect to them. For more information

regarding the servers deployment, please read the Installing DeviceLock Enterprise Server and Installing DeviceLock Content Security Server sections of this manual.

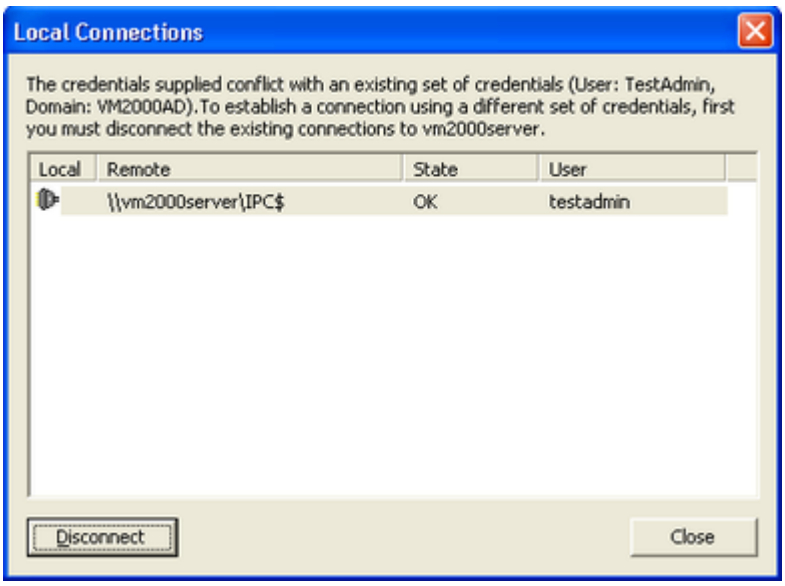
If you don't have administrative privileges on the selected computer, DeviceLock Management Console suggests that you connect under the account of another user.



In the **User name** parameter you can specify a user account with administrative privileges. This account should also be on the list of DeviceLock Administrators in case this administrator safeguard feature is enabled for DeviceLock Service or DeviceLock Enterprise Server or DeviceLock Content Security Server.

A "credentials conflict" can result if, after connecting to (i.e., you have a mapped network disk, opened shared resource, etc.) a selected computer under a user that can't access DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server, you then try to login as another user in DeviceLock Management Console. To avoid this conflict you must first delete your existing connection.

When DeviceLock Management Console detects a credentials conflict it displays a list of existing connections on your local computer and suggests that you delete some of them.


Local Connections
The credentials supplied conflict with an existing set of credentials (User: TestAdmin, Domain: VM2000AD). To establish a connection using a different set of credentials, first you must disconnect the existing connections to vm2000server.
Local
Remote
State
User
\\vm2000server\IPC$
OK
testadmin
Disconnect
Close

Highlight all existing connections to the computer you want to connect to and press the **Disconnect** button.

Press the **Close** button and then try to connect to this computer again.

Note: Sometimes the existing connection can't be terminated thus preventing you from connecting under a different user account in DeviceLock Management Console. In this case you need to run DeviceLock Management Console under a user that either has sufficient privileges to access DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server or has no connections to the selected computer at all. You may use the Run As function (run RUNAS from the command line) available in Windows 2000 and later to run DeviceLock Management Console under another user.

Possible Connection Errors

When you're trying to connect to a computer with DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server you may receive some of these errors:

- **(1722) The RPC server is unavailable** – you're trying to connect to a computer that either does not exist (the wrong name or IP address) or is not accessible. Make sure that the computer name you've specified is correct. Try to ping this computer by its name and IP address and connect to it using any standard Windows administrative tool (such as Computer Management, Services and so on). Make sure that this computer is working under a DeviceLock-compatible OS (Windows NT 4.0 and later).

  Also, it is possible that a firewall is blocking access to this computer. You would need to configure your firewall to allow some ports needed for DeviceLock. You could also instruct DeviceLock to use the fixed TCP port, making it easier to configure a firewall. By default, DeviceLock Service, DeviceLock Enterprise Server and DeviceLock

Content Security Server are using 9132, 9133 and 9134 ports thereafter. For more information, please refer to the Frequently Asked Questions section of our Web site. Also, please note that DeviceLock Service automatically adds itself to the exception list of Windows Firewall.

- **(1753) There are no more endpoints available from the endpoint mapper** – you're trying to connect to a computer where DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server is not accessible. First of all, make sure that DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server is installed and started on the remote computer.

  It is possible that this computer was just booted and Windows is still initializing its services. The Remote Procedure Call (RPC) service may not be running yet.

  Also, a firewall could be blocking access to DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server. For more information, please read the above description of the 1722 error.

  To troubleshoot RPC Endpoint Mapper errors, please read this Microsoft article: support.microsoft.com/kb/839880/en-us.

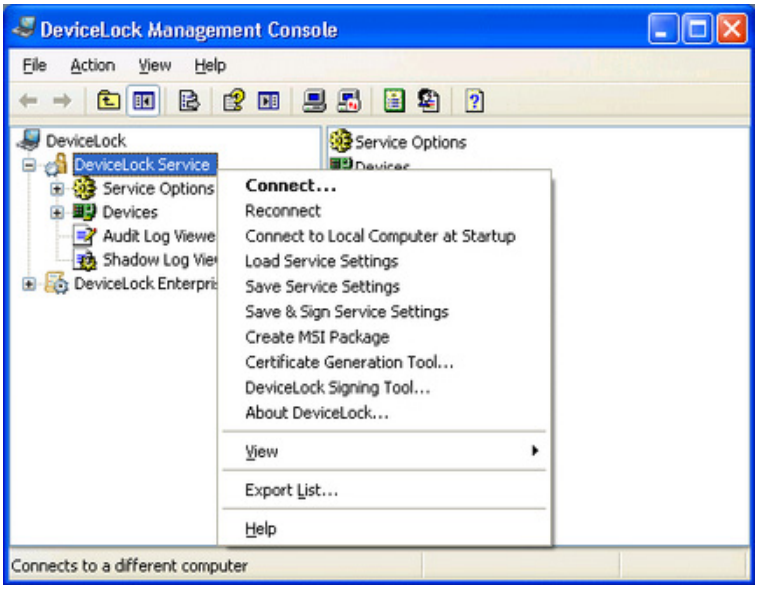
- **(5) Access is denied** – you don't have enough privileges on the remote computer. Make sure that DeviceLock Management Console is trying to connect to the remote computer under a user with local administrator privileges on that computer.

  You may also need to run DeviceLock Management Console under a different user that can authenticate on the remote computer as a local admin.

- **(7045) You must have administrative privileges to perform this operation** – you don't have sufficient privileges to access DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server because the user is not in the list of DeviceLock Administrators. Make sure that DeviceLock Management Console is trying to connect to the remote computer under the user that is in the list of DeviceLock Administrators on that computer.

Managing DeviceLock Service for Windows

Expand the **DeviceLock Service** item to access all of the service function and configuration parameters.



There is a context menu available via a right mouse click on the **DeviceLock Service** item:

- **Connect** – connects to any computer that you specify. For more information please read the Connecting to Computers section of this manual.
- **Reconnect** – connects to the currently connected computer once again.
- **Connect to Local Computer at Startup** – check this flag to instruct DeviceLock Management Console to automatically connect to the local computer each time it starts up.
- **Undefine ContentLock policy** – resets all ContentLock's parameters (all Content-Aware Rules except those based on file types) to the unconfigured state in one click.
- **Undefine NetworkLock policy** – resets all NetworkLock's parameters to the unconfigured state in one click.
- **Load Service Settings** – loads previously saved settings from the XML file and applies these settings to the currently connected DeviceLock Service. You need to select the file that was created either by DeviceLock Service Settings Editor, DeviceLock Management Console or DeviceLock Group Policy Manager. Since the signature is not validated at this step, it can be either a signed or non-signed file.
- **Save Service Settings** – exports all settings from the currently connected DeviceLock Service to an external XML file. Later this file can be modified using DeviceLock Service Settings Editor and loaded via DeviceLock Management Console and/or DeviceLock Group Policy Manager. Also, this file can be sent to users whose computers are not online and thus out-of-reach via management consoles. To avoid unauthorized modification the file should be signed with the DeviceLock Certificate (the private key) using the DeviceLock Signing Tool.

- **Save & Sign Service Settings** – exports all settings from the currently connected DeviceLock Service to an external XML file and automatically signs it with the most recent DeviceLock Certificate (the private key). This menu item is disabled when the DeviceLock Signing Tool has no previously loaded private key.
- **Certificate Generation Tool** – runs the special tool that allows you to generate DeviceLock Certificates. For more information please read the Generating DeviceLock Certificates section of this manual.
- **Create MSI Package** – creates the custom Microsoft Software Installer (MSI) package with settings from the currently connected DeviceLock Service.

  At the first step you need to select the source MSI package with DeviceLock Service. You may use MSI packages that ship with DeviceLock (such as DeviceLock Service.msi and DeviceLock Service x64.msi).

  Then you need to specify the name of the resultant (target) MSI package that will be generated based on the source MSI package (specified at the first step) and settings from the currently connected DeviceLock Service.

  Later this custom MSI package can be used to deploy DeviceLock Service instances across the network with predefined policies. For more information on how to deploy DeviceLock Service using MSI, please read the Installation via Group Policy section of this manual.

  Note: If you use a custom MSI package with defined DeviceLock Service settings to deploy DeviceLock Service using Group Policy, these settings are not applied to client computers if any one of the following conditions is true:

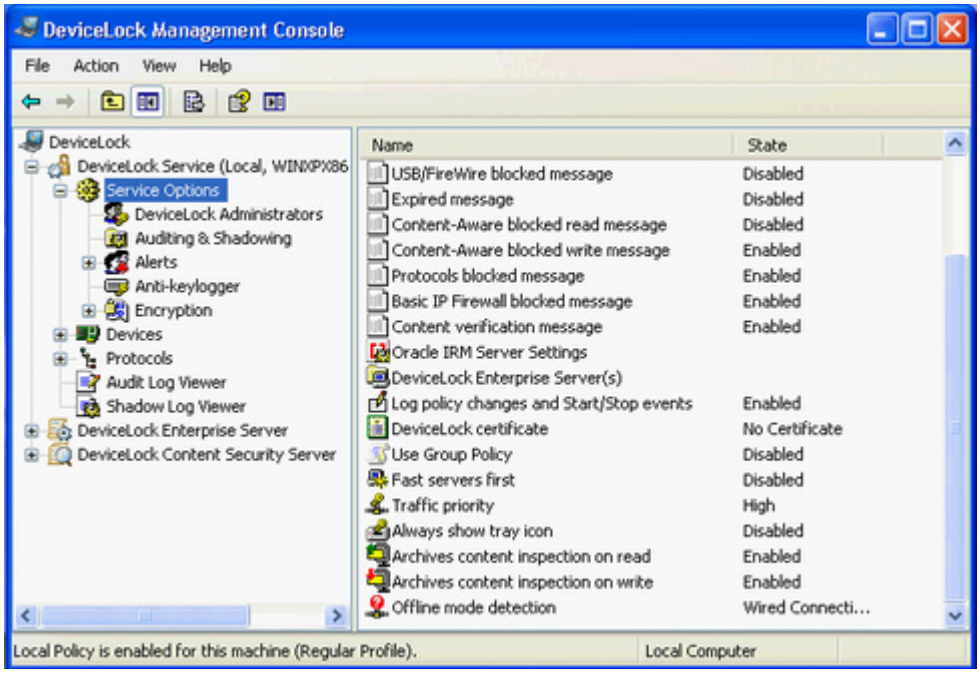
  - The default security is disabled on remotely running DeviceLock Services.
  - The GPO applied to client computers has the **Override Local Policy** setting enabled.

  Please note that the **Create MSI Package** menu item is disabled when there is no Microsoft Windows Installer (version 1.0 or later) installed on the local computer.

- **DeviceLock Signing Tool** – runs the special tool that allows you to grant users temporary access to requested devices and sign XML files with DeviceLock Service settings. For more information please read the DeviceLock Signing Tool section of this manual.
- **About DeviceLock** – displays a dialog box with information about the DeviceLock version and your licenses.

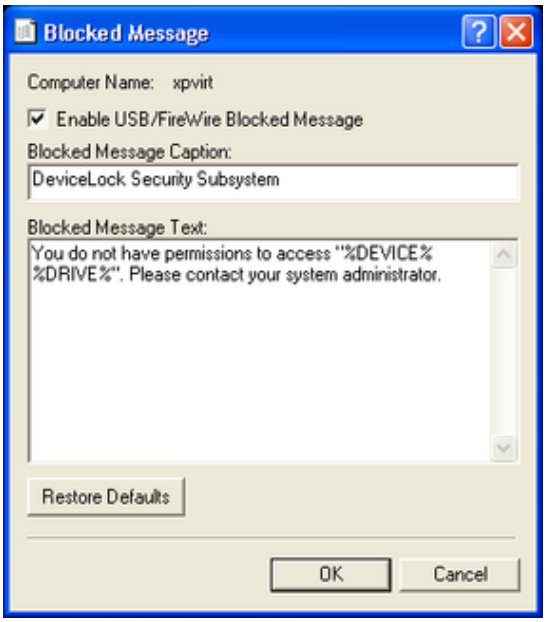
Service Options

These additional parameters allow you to tune up the DeviceLock Service configuration. Use the context menu available by a right mouse click on every parameter.



USB/FireWire blocked message

You can define a custom message to be displayed to users when a USB or FireWire device that is denied at the interface (USB or FireWire) level or type (Removable, Optical Drive, etc.) level is plugged in.



To enable this custom message, select the **Enable USB/FireWire Blocked Message** check box.

Also, you can define additional parameters, such as:

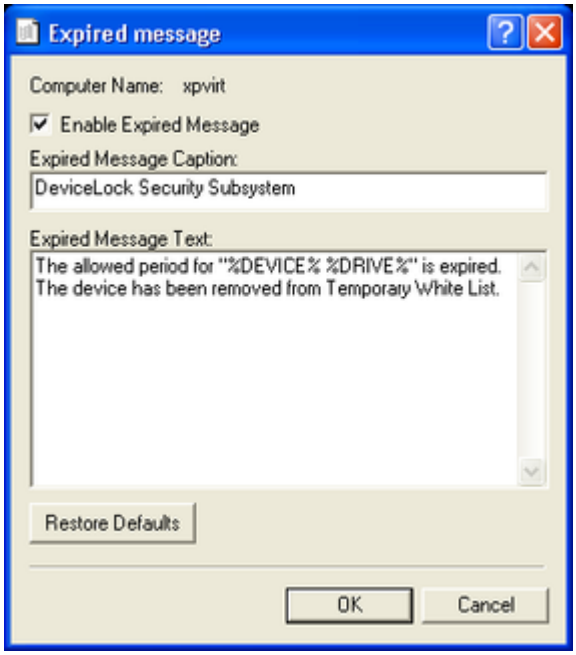
- **Blocked Message Caption** – the text to be displayed as a caption. You can use three predefined macros within the text:
  - **%TYPE%** – inserts the port name (USB port, FireWire port) where the device is plugged.
  - **%DEVICE%** – inserts the name of the device (e.g. USB Mass Storage Device) received from the system.
  - **%DRIVE%** – inserts the drive letter of the storage device (e.g. F:). If the device doesn't have a letter, then this macro inserts an empty string.

  Using these macros you can create more informative messages for users.

- **Blocked Message Text** – the main text of the message. You can use the predefined macros described above within the text.

Expired message

You can define a custom message to be displayed to users when the allowed period for temporary white listed devices is expired and devices have been removed from Temporary White List.



To enable this custom message, select the **Enable Expired Message** check box.

Also, you can define additional parameters, such as:

- **Expired Message Caption** – the text to be displayed as a caption. You can use two predefined macros within the text:
  - **%DEVICE%** – inserts the name of the device (e.g. USB Mass Storage Device) received from the system.

- **%DRIVE%** – inserts the drive letter of the storage device (e.g. F:). If the device doesn't have a letter, then this macro inserts an empty string.

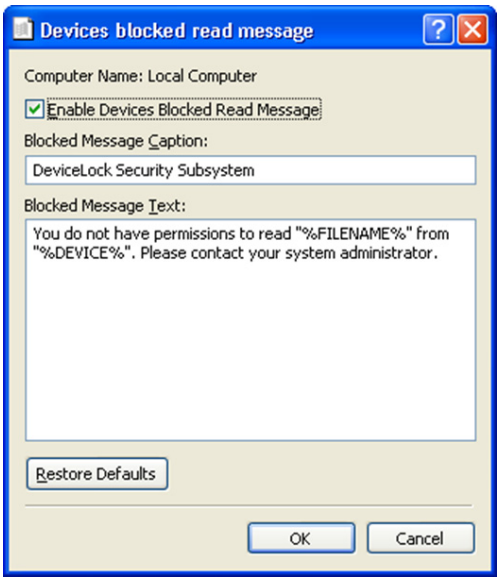
Using these macros you can create more informative messages for users.

- **Expired Message Text** – the main text of the message. You can use the predefined macros described above within the text.

Devices blocked read message

You can define a custom message to be displayed to users when read access to Floppy, Hard disk, Optical Drive, Removable, Tape, MTP, iPhone, Palm, and Windows Mobile devices, as well as access to TS Devices (Clipboard Incoming Text, Clipboard Incoming Image, Clipboard Incoming Audio, Clipboard Incoming File, Clipboard Incoming Unidentified Content) is denied.

Note: The message is also displayed to users when read or write access to Blackberry, Bluetooth, FireWire, Infrared, Serial and Parallel ports, TS Devices (USB Port and Serial Port), USB Port, and WiFi is denied.


Devices blocked read message
Computer Name: Local Computer
Enable Devices Blocked Read Message
Blocked Message Caption:
DeviceLock Security Subsystem
Blocked Message Text:
You do not have permissions to read "%FILENAME%" from "%DEVICE%". Please contact your system administrator.
Restore Defaults
OK
Cancel

To enable this custom message, select the **Enable Devices Blocked Read Message** check box.

Note: The message is displayed to the user whose access rights lack read access permissions at the very moment an attempt to gain read access is made. In some cases, if terminal server sessions are in use, the message may be displayed to all users who are logged in to the terminal server.

When read or write access to WiFi or Bluetooth are denied, the message is only displayed once. There will be no further messages until the appropriate settings are modified.

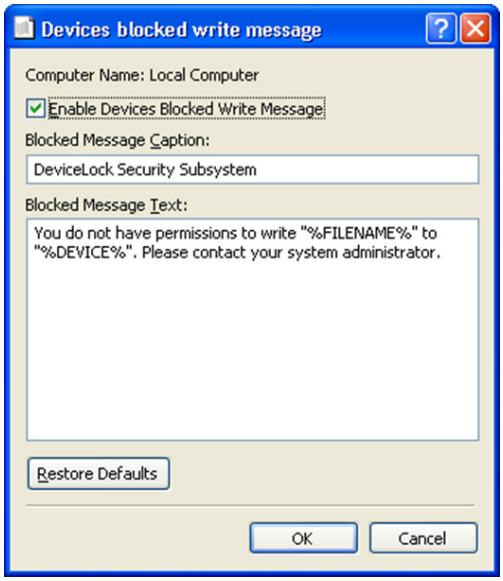
Also, you can define additional parameters, such as:

- **Blocked Message Caption** – the text to be displayed as a caption. You can use two predefined macros within the text:
  - **%FILENAME%** – inserts the name of the file to be read.
  - **%DEVICE%** – inserts the name of the device (e.g. USB Mass Storage Device) received from the system.

    Using these macros you can create more informative messages for users.
- **Blocked Message Text** – the main text of the message. You can use the predefined macros described above within the text.

Devices blocked write message

You can define a custom message to be displayed to users when write access to Floppy, Hard disk, Optical Drive, Removable, Tape, MTP, iPhone, Palm, Windows Mobile devices, Clipboard (Copy text, Copy Image, Copy Audio, Copy File, Copy Unidentified Content), and Printer devices, as well as access to TS Devices (Clipboard Outgoing Text, Clipboard Outgoing Image, Clipboard Outgoing Audio, Clipboard Outgoing File, Clipboard Outgoing Unidentified Content) is denied.


Devices blocked write message
Computer Name: Local Computer
Enable Devices Blocked Write Message
Blocked Message Caption:
DeviceLock Security Subsystem
Blocked Message Text:
You do not have permissions to write "%FILENAME%" to "%DEVICE%". Please contact your system administrator.
Restore Defaults
OK
Cancel

To enable this custom message, select the **Enable Devices Blocked Write Message** check box.

Note: The message is displayed to the user whose access rights lack write access at the very moment an attempt to gain write access is made. In some cases, in terminal sessions, the message may be displayed to all users who logged in to the terminal server.

The message is not displayed to users when write access to Blackberry, Bluetooth, FireWire, Infrared, Serial and Parallel ports, TS Devices (USB Port and Serial Port), USB Port, and WiFi is denied. **Devices Blocked Read Message** is displayed in these cases.

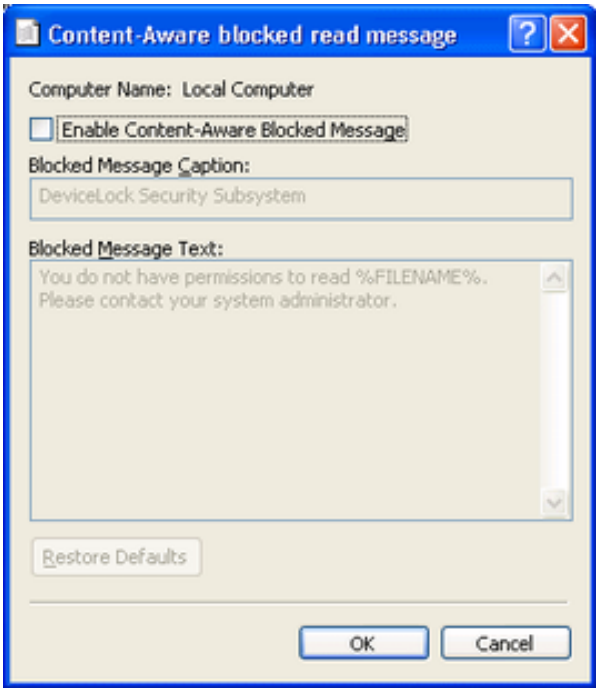
Also, you can define additional parameters, such as:

- **Blocked Message Caption** – the text to be displayed as a caption. You can use two predefined macros within the text:
  - **%FILENAME%** – inserts the name of the file to be written.
  - **%DEVICE%** – inserts the name of the device (e.g. USB Mass Storage Device) received from the system.
    Using these macros you can create more informative messages for users.
- **Blocked Message Text** – the main text of the message. You can use the predefined macros described above within the text.

Content-Aware Blocked Read Message

You can define a Content-Aware blocked read message (notification balloon) to be displayed to users when they try to read a file to which they are denied access. This message balloon is shown in the notification area of the taskbar on client computers. By default, DeviceLock does not display the Content-Aware blocked read message.

To enable or disable the Content-Aware blocked read message, right-click **Content-Aware blocked read message** and then click **Properties**, or double-click **Content-Aware blocked read message**.



In the **Content-Aware blocked read message** dialog box, do the following:

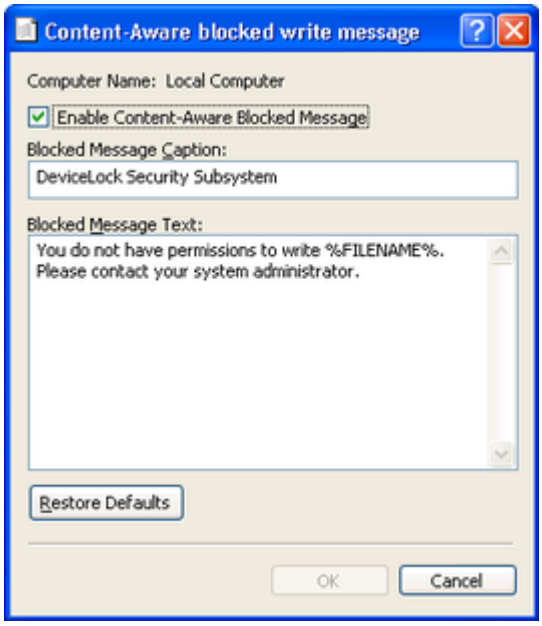
USE THIS	TO DO THIS
Enable Content-Aware Blocked Message	Enable or disable the display of the Content-Aware blocked read message. Select the **Enable Content-Aware Blocked Message** check box to enable the display of the message. Clear the **Enable Content-Aware Blocked Message** check box to disable the display of the message.
Blocked Message Caption	Specify the text to display in the title bar of the message balloon. By default, the Blocked Message Caption text is as follows: **DeviceLock Security Subsystem**
Blocked Message Text	Specify the text to display in the message balloon. By default, the Blocked Message Text for the Content-Aware blocked read message is as follows: **You do not have permissions to read "%FILENAME%". Please contact your system administrator.** where **%FILENAME%** is the path and file name of the file to be inserted.
Restore Defaults	Restore the default settings.

For a detailed description of the Content-Aware Rules feature, see "Content-Aware Rules for Devices (Regular Profile)" and "Content-Aware Rules for Protocols (Regular Profile)."

Content-Aware Blocked Write Message

You can define a Content-Aware blocked write message (notification balloon) to be displayed to users when they try to write a file or transfer the data to which they are denied access. This message balloon is shown in the notification area of the taskbar on client computers. By default, DeviceLock displays the Content-Aware blocked write message.

To enable or disable the Content-Aware blocked write message, right-click **Content-Aware blocked write message** and then click **Properties**, or double-click **Content-Aware blocked write message**.



In the **Content-Aware blocked write message** dialog box, do the following:

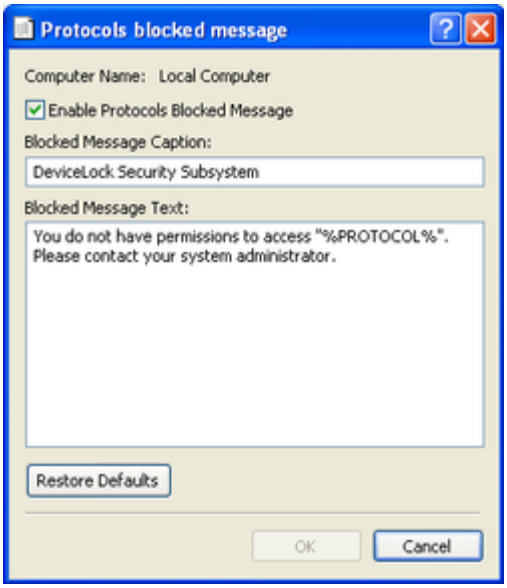
USE THIS	TO DO THIS
Enable Content-Aware Blocked Message	Enable or disable the display of the Content-Aware blocked write message. Select the **Enable Content-Aware Blocked Message** check box to enable the display of the message. Clear the **Enable Content-Aware Blocked Message** check box to disable the display of the message.
Blocked Message Caption	Specify the text to display in the title bar of the message balloon. By default, the Blocked Message Caption text is as follows: **DeviceLock Security Subsystem**
Blocked Message Text	Specify the text to display in the message balloon. By default, the Blocked Message Text for the Content-Aware blocked write message is as follows: **You do not have permissions to send data/file "%FILENAME%" via "%CHANNEL_NAME%". Please contact your system administrator.** where **%FILENAME%** is the path and file name of the file to be inserted; **%CHANNEL_NAME%** is a data transmission channel to be inserted.
Restore Defaults	Restore the default settings.

For a detailed description of the Content-Aware Rules feature, see "Content-Aware Rules for Devices (Regular Profile)" and "Content-Aware Rules for Protocols (Regular Profile)."

Protocols blocked message

You can define a Protocols blocked message (notification balloon) to be displayed to users when they try to access a protocol to which they are denied access. This message balloon is shown in the notification area of the taskbar on client computers.

To enable or disable the Protocols blocked message, right-click **Protocols blocked message**, and then click **Properties**, or double-click **Protocols blocked message**.



In the **Protocols blocked message** dialog box, do the following:

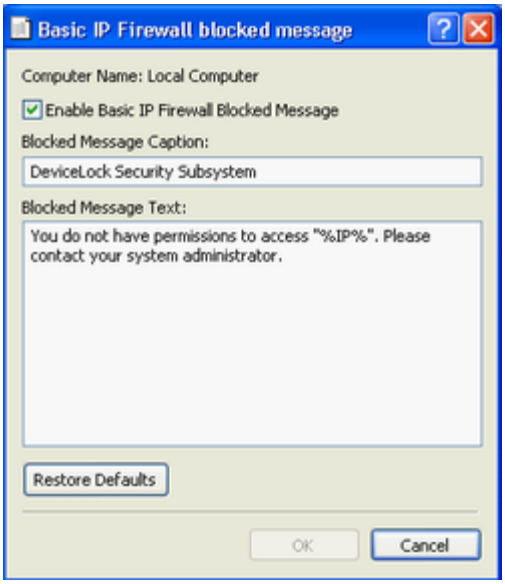
USE THIS	TO DO THIS
Enable Protocols Blocked Message	Enable or disable the display of the Protocols blocked message. Select the **Enable Protocols Blocked Message** check box to enable the display of the message. Clear the **Enable Protocols Blocked Message** check box to disable the display of the message.
Blocked Message Caption	Specify the text to display in the title bar of the message balloon. By default, the Blocked Message Caption text is as follows: **DeviceLock Security Subsystem**
Blocked Message Text	Specify the text to display in the message balloon. By default, the Blocked Message Text is as follows: **You do not have permissions to access %PROTOCOL%. Please contact your system administrator.** where **%PROTOCOL%** is the name of the protocol to be inserted.
Restore Defaults	Restore the default settings.

For a detailed description of the Protocols feature, see "Protocols (Regular Profile)."

Basic IP Firewall blocked message

You can define a Basic IP Firewall blocked message to be displayed to users when they try to establish a connection to which they are denied access.

To enable or disable the Basic IP Firewall blocked message, right-click **Basic IP Firewall blocked message**, and then click **Properties**, or double-click **Basic IP Firewall blocked message**.


Basic IP Firewall blocked message
Computer Name: Local Computer
Enable Basic IP Firewall Blocked Message
Blocked Message Caption:
DeviceLock Security Subsystem
Blocked Message Text:
You do not have permissions to access "%IP%". Please contact your system administrator.
Restore Defaults
OK
Cancel

In the **Basic IP Firewall blocked message** dialog box, do the following:

USE THIS	TO DO THIS
Enable Basic IP Firewall Blocked Message	Enable or disable the display of the Basic IP Firewall blocked message. Select the **Enable Basic IP Firewall Blocked Message** check box to enable the display of the message. Clear the **Enable Basic IP Firewall Blocked Message** check box to disable the display of the message.
Blocked Message Caption	Specify the text to display in the title bar of the message box. By default, the Blocked Message Caption text is as follows: **DeviceLock Security Subsystem**

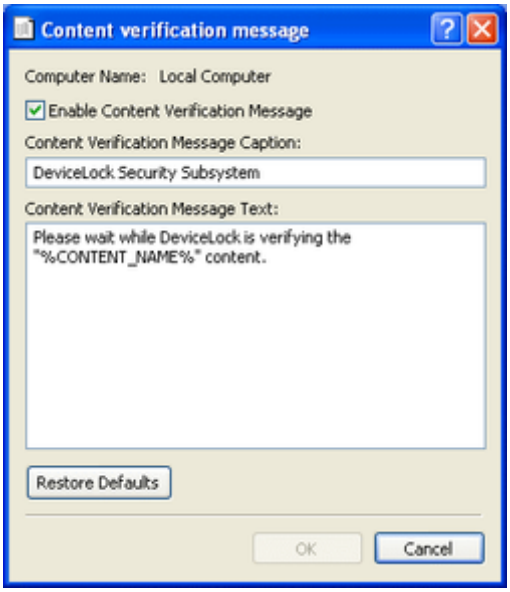
USE THIS	TO DO THIS
Blocked Message Text	Specify the text to display in the message box. By default, the Blocked Message Text is as follows: **You do not have permissions to access %IP%. Please contact your system administrator.** where **%IP%** is the IP address of the host to be inserted.
Restore Defaults	Restore the default settings.

For a detailed description of the Basic IP Firewall feature, see "Managing Basic IP Firewall."

Content verification message

Checking the content of files copied to devices or transmitted over the network can be a time-consuming operation. You can define a Content verification message to be displayed to users when content inspection is in progress. This message is displayed 20 seconds after DeviceLock Service starts checking the file content.

To enable or disable the Content verification message, right-click **Content verification message**, and then click **Properties**, or double-click **Content verification message**.



In the **Content verification message** dialog box, do the following:

USE THIS	TO DO THIS
Enable Content Verification Message	Enable or disable the display of the Content verification message. Select the **Enable Content Verification Message** check box to enable the display of the message.

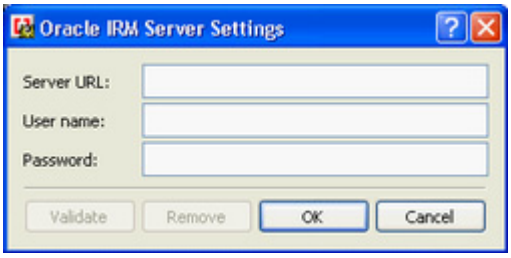
USE THIS	TO DO THIS
	Clear the **Enable Content Verification Message** check box to disable the display of the message.
Content Verification Message Caption	Specify the text to display in the title bar of the message box. By default, the Content Verification Message Caption text is as follows: **DeviceLock Security Subsystem**
Content Verification Message Text	Specify the text to display in the message box. By default, the Content Verification Message Text is as follows: **Please wait while DeviceLock is verifying the %CONTENT_NAME% content**. where **%CONTENT_NAME%** is the name of the file or protocol to be inserted. The file name is inserted when DeviceLock checks the content of files copied to a device. The protocol name is inserted when DeviceLock checks the content of data transmitted over the network.
Restore Defaults	Restore the default settings.

For a detailed description of the Content-Aware Rules feature, see "Content-Aware Rules for Devices (Regular Profile)" and "Content-Aware Rules for Protocols (Regular Profile)."

Oracle IRM Server Settings

Use this option to configure DeviceLock Service for Oracle IRM support. If you have configured Oracle IRM support, you can define Content-Aware Rules to control access to documents that have been sealed using IRM.

Configuration settings are specified in the **Oracle IRM Server Settings** dialog box. To open this dialog box, right-click **Oracle IRM Server Settings**, and then click **Properties**, or double-click **Oracle IRM Server Settings**.



In the **Oracle IRM Server Settings** dialog box, do the following:

USE THIS	TO DO THIS
Server URL	Specify the URL of the IRM server used to seal documents for which you want to control access.

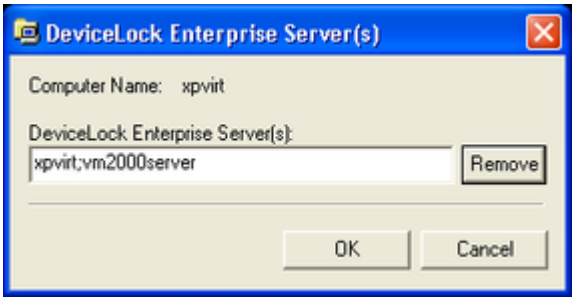
USE THIS	TO DO THIS
User name	Specify the user account to use for authentication with the IRM server.
Password	Specify the password corresponding to the user account to use for authentication with the IRM server.
Validate	Contact the specified IRM server and validate user name/password as well as the URL against the one configured on the IRM Server.
Remove	Remove the specified IRM server.

When configuring DeviceLock Service for Oracle IRM support, consider the following:

- The required IRM server must be installed and be accessible for DeviceLock Service.
- You must install Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0 on the IRM server. You can download them from the Oracle Web site.
- The IRM server you want to use must have a "device count" greater than 1.
- The IRM server certificate name must coincide with the IRM server name.

DeviceLock Enterprise Server(s)

If you want to allow DeviceLock Service to send its logs to DeviceLock Enterprise Server, specify the name or IP address of this server's computer.



Using the semicolon (;) as a separator you can specify several DeviceLock Enterprise Servers to uniformly spread the network load. At its startup, DeviceLock Service chooses one server for sending logs. If the selected server is unavailable, DeviceLock Service tries to choose another one from the list.

Make sure that DeviceLock Enterprise Server is properly installed and accessible for DeviceLock Service, otherwise logs will not be stored in the centralized database. For more information on how to install DeviceLock Enterprise Server, please read the Installing DeviceLock Enterprise Server section of this manual.

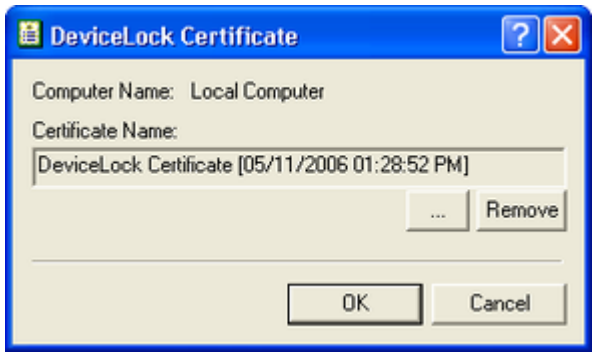
Log Policy changes and Start/Stop events

You can enable the logging of changes in the DeviceLock Service's configuration and report the time when DeviceLock Service starts and stops. It is possible to log changes in permissions, audit rules, white lists and in other settings.

To allow this logging, enable the **Log Policy changes and Start/Stop events** parameter.

DeviceLock Certificate

Use this parameter to install or remove a DeviceLock Certificate.



Specify the path to the public key in the **Certificate Name** parameter if you want to install the certificate. You can use the **...** button to select the file with a public key.

To remove the public key, use the **Remove** button.

For more information about DeviceLock Certificates, please read the DeviceLock Certificates section of this manual.

Use Group Policy

If DeviceLock Service is configured to work with Group Policy in an Active Directory domain, you can control the effective policy mode (Group Policy or Local Policy).

To activate the Group Policy mode for this DeviceLock Service, enable the **Use Group Policy** parameter. In this mode, all settings that you set via DeviceLock Management Console and DeviceLock Enterprise Manager are replaced by Group Policy settings.

To activate the Local Policy mode for this DeviceLock Service, disable the **Use Group Policy** parameter. In this mode, all settings that you set via DeviceLock Management Console and DeviceLock Enterprise Manager have a priority over Group Policy settings and replace them.

If DeviceLock Service was not configured to work with Group Policy, the **Use Group Policy** parameter is disabled and unavailable for changing.

If the **Use Group Policy** parameter is enabled but unavailable for changing, it means that the Group Policy mode always has a priority (the **Override Local Policy** parameter was enabled in DeviceLock Group Policy Manager) and the Local Policy mode can't be enabled for this DeviceLock Service. For more information, please read the Using DeviceLock Group Policy Manager section of this manual.

Fast servers first

DeviceLock Service can choose the fastest available DeviceLock Enterprise Server from the list of servers.

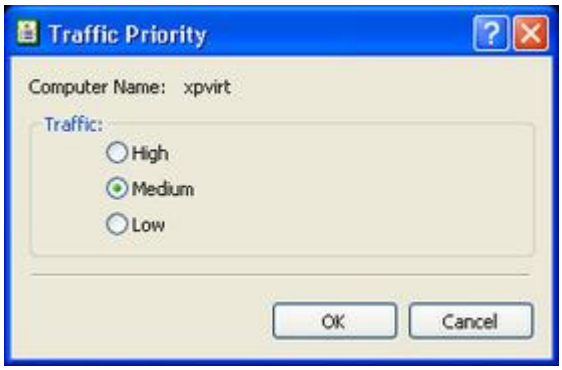
When this parameter is enabled, all servers specified in the **DeviceLock Enterprise Server(s)** parameter are divided into three groups depending on their network speed and preference is given to the fastest. If all of the fastest servers are unavailable, DeviceLock Service attempts to select a server from the group of next fastest servers and so on.

If the **Fast servers first** parameter is disabled, DeviceLock Service randomly selects a server from the list.

This parameter has an effect only if there is more than one server specified in the **DeviceLock Enterprise Server(s)** parameter.

Traffic priority

DeviceLock supports traffic shaping, allowing you to define bandwidth limits for sending audit and shadow logs from DeviceLock Service to DeviceLock Enterprise Server.



You can set three types of traffic priority: high, medium and low.

When **High** is selected it means that 100% of bandwidth can be used. To allow use of only up to 50% of bandwidth, select **Medium**. Select **Low** to allow use of just up to 10% of bandwidth.

Please note that medium and low priorities have an effect only if the Quality of Service Packet Scheduler (QoS Packet Scheduler) component is installed on a computer running DeviceLock Service. Otherwise, the **Traffic priority** parameter is disabled and 100% of bandwidth is used. For more information on QoS, please refer to Microsoft's on-line article.

Always show tray icon

Use this option to enable or disable the display of the DeviceLock Tray Notification Utility icon in the notification area of the taskbar on client computers. End users working on client

computers can refresh the connection state (online or offline) of DeviceLock Service. To do so, they need to right-click the DeviceLock Tray Notification Utility icon in the notification area of the taskbar, and then click **Refresh Current State**. There are three icons for DeviceLock Tray Notification Utility:

- – means that DeviceLock works in the online mode (the regular profile is used).
- – means that DeviceLock works in the offline mode (the offline profile is used).
- – means that DeviceLock detects its connection state (the previous state profile is used).

End users can click the DeviceLock Tray Notification Utility icon to view the latest DeviceLock message balloon shown for the notification in the notification area of a client computer.

End users can also use **Show Message History** option that displays all notifications since the last start-up of the DeviceLock Service.

To enable or disable the display of the DeviceLock Tray Notification Utility icon, right-click **Always show tray icon** and then click **Enable**/**Disable**, or double-click **Always show tray icon**.

Archives content inspection on read

Use this option to enable or disable content inspection of files within archives when users try to read archive files. For more information, see the description of the Inspection of files within archives feature. To enable or disable content inspection of files within archives, right-click **Archives content inspection on read** and then click **Enable**/**Disable**, or double-click **Archives content inspection on read**.

Note: If this option is disabled, inspection of documents embedded in saved emails (EML), Adobe Portable Document Format (PDF) files, Rich Text Format (RTF), AutoCAD files (.dwg, .dxf), and Microsoft Office documents (.doc, .xls, .ppt, .docx, .xlsx, .pptx) is also not performed.

Archives content inspection on write

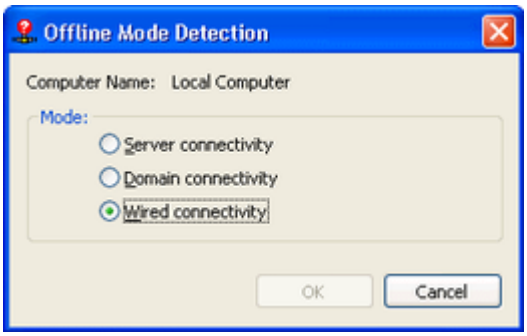
Use this option to enable or disable content inspection of files within archives when users try to write archive files. For more information, see the description of the Inspection of files within archives feature. To enable or disable content inspection of files within archives, right-click **Archives content inspection on write** and then click **Enable**/**Disable**, or double-click **Archives content inspection on write**.

Note: If this option is disabled, inspection of documents embedded in saved emails (EML), Adobe Portable Document Format (PDF) files, Rich Text Format (RTF), AutoCAD files (.dwg, .dxf), and Microsoft Office documents (.doc, .xls, .ppt, .docx, .xlsx, .pptx) is also not performed.

Offline mode detection

Use this option to configure offline mode detection settings. You can define the network characteristics that DeviceLock uses to detect its connection state (whether it is online or offline). By default, DeviceLock works in offline mode when the network cable is not connected to the client computer.

To configure offline mode detection settings, right-click **Offline mode detection** and then click **Properties**, or double-click **Offline mode detection**.



You can choose any of the following options:

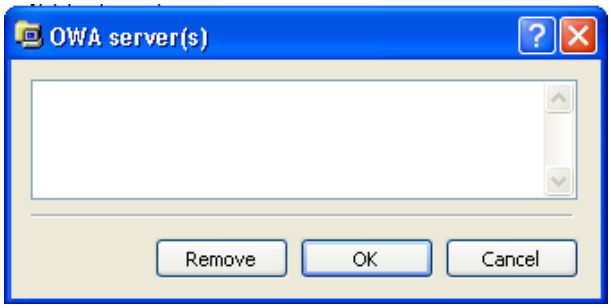
OPTION	DESCRIPTION
Server connectivity	Indicates that the connection state of a client computer is determined by whether or not it can connect to the specified DeviceLock Enterprise Server. Thus, a client computer works in online mode, if it can connect to any of the specified DeviceLock Enterprise Servers and send them audit and shadow logs. A client computer works in offline mode if it cannot authenticate with any of the specified DeviceLock Enterprise Servers or all of the specified DeviceLock Enterprise Servers become unavailable at the same time. **Best Practice:** The most reliable way to secure client/server communication is to use DeviceLock Certificate authentication. For client/server certificate authentication, the public key must be installed on client computers, while the private key must be installed on DeviceLock Enterprise Server(s). If the certificate (the public key) is installed only on client computers, the server will reject connections and client computers will work in offline mode. If the certificate (the private key) is installed only on DeviceLock Enterprise Server, the server and the client will authenticate each other once a connection is established though this type of authentication is less secure than certificate-based authentication. For detailed information on DeviceLock Certificates, see "DeviceLock Certificates."

OPTION	DESCRIPTION
Domain connectivity	Indicates that the connection state of a client computer is determined by whether or not it can connect to the appropriate Active Directory domain controller (a domain controller of the domain to which the client computer belongs). Thus, a client computer works in online mode, if it can connect to the appropriate domain controller. A client computer works in offline mode, if the appropriate domain controller becomes unavailable. *A client computer that is not joined to a domain (a workgroup or stand-alone computer) always works in offline mode.*
Wired connectivity	Indicates that the connection state of a client computer is determined by whether or not the network cable is connected to the Network Interface Card (NIC). This is the simplest and least secure method of detecting the connection state. Thus, a client computer works in online mode, if the network cable is connected to the NIC. A client computer works in offline mode, if the network cable is disconnected from the NIC. Please note that wireless network connections (WiFi, etc.) and modem connections are ignored. This option is selected by default.

For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)."

OWA server(s)

This parameter allows you to define the list of Outlook Web App (OWA, originally called Outlook Web Access) server's URLs. OWA servers specified here are treated as the Web Mail protocol by the NetworkLock module. All OWA servers not specified here are treated as the HTTP protocol by the NetworkLock module.



Multiple URLs must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry.

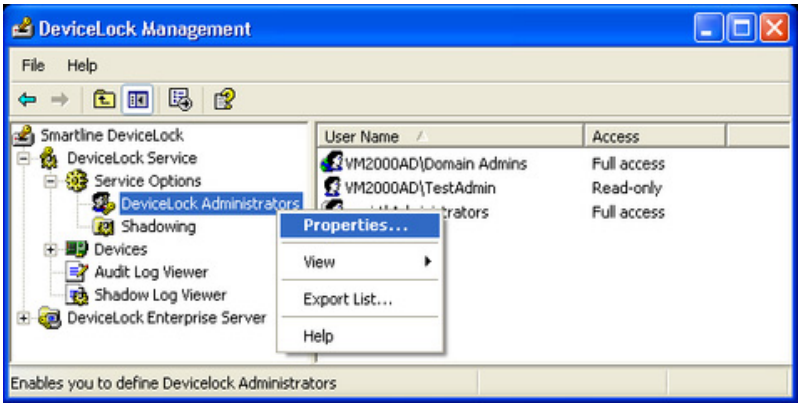
You can use the asterisk (*) wildcard character in URLs (for example, ***.com/owa** denotes that the URL is any server whose name ends in the specified name).

Apply Content-Aware Rules to file/folder names

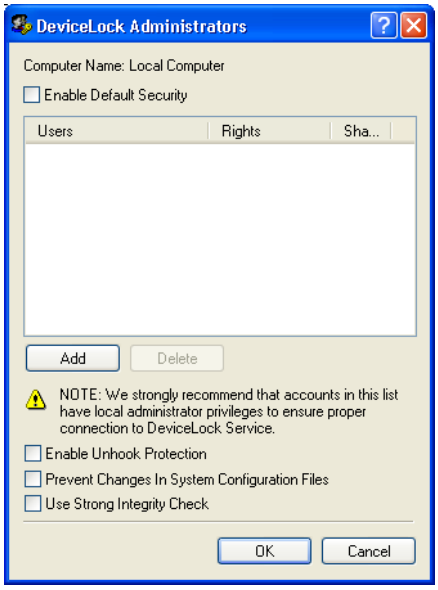
Use this option to enable or disable content inspection of file and folder names when users try to access, create, or rename files and folders for managed storage-based device types. Only rules based on Pattern and Keywords groups may be applied to file and folder names. Rules apply to the full file/folder path.

DeviceLock Administrators

This parameter allows you to define the list of user accounts with administrative access rights to DeviceLock Service.



Use the context menu available by a right mouse click on the **DeviceLock Administrators** item to open the configuration dialog box.



DeviceLock's default security configuration is based on Windows Access Control Lists (ACL). A user without administrative privileges can't connect to DeviceLock Service, modify its settings or remove it. Everything is controlled by the Windows security subsystem.

To turn on the default security based on Windows ACL, select the **Enable Default Security** check box.

Note: As described in the Recommended Basic Security Measures section of this manual, giving administrative privileges to regular users is strongly discouraged.

Users with local administrator privileges (i.e. members of the local Administrators group) can connect to DeviceLock Service using a management console and change permissions, auditing and other parameters. Moreover, such users can uninstall DeviceLock from their computers, disable or delete DeviceLock Service, modify a service's registry keys, delete a service's executable file, and so on. In other words, users with local administrator privileges can circumvent the default security based on Windows ACL.

However, if for some reason, users in your network have administrator privileges on their local computers, DeviceLock does provide another level of protection – DeviceLock Security. When DeviceLock Security is enabled, no one except authorized users can connect to DeviceLock Service or stop and uninstall it. Even members of the local Administrators group (if they are not on the list of authorized DeviceLock administrators) can't circumvent DeviceLock Security.

To turn on DeviceLock Security, clear the **Enable Default Security** check box.

Then you need to specify authorized accounts (users and/or groups) that can administer DeviceLock Service. To add a new user or user group to the list of accounts, click the **Add** button. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the **Delete** button. Using Ctrl and/or Shift you can highlight and remove several records simultaneously.

To define which DeviceLock administrative actions are to be allowed for a user or user group, set the appropriate rights:

- **Full access** – to enable full access to DeviceLock Service. Users can modify permissions, auditing and other parameters, remove and update DeviceLock Service.
- **Change** – to enable change access to DeviceLock Service. Users can change settings, install, and uninstall DeviceLock Service, but they cannot add new users to the list of authorized accounts that can administer DeviceLock Service or change access rights for existing users in this list.
- **Read-only** – to enable only the reading of permissions, auditing and other parameters. Users can run reports, view defined parameters but cannot modify anything or remove/update DeviceLock Service.
- **Shadow Data Access** – to enable access to shadowed data. Users can open, view and download shadow data using service's shadow log viewer.

Note: We strongly recommend that accounts included in this list have local administrator privileges because, in some instances, installing, updating and uninstalling DeviceLock Service may require access rights to Windows Service Control Manager (SCM) and shared network resources.

Here is just one example of how to properly define a DeviceLock Administrators list: add a Domain Admins group with **Full access** rights. Because Domain Admins is a member of the local group Administrators on every computer in the domain, all members of Domain Admins will have full access to DeviceLock Service on every computer. However, other members of the local group Administrators will not be able to administer DeviceLock Service or disable it.

Also, by selecting the **Enable Unhook Protection** check box, you can turn on optional protection against anti-rootkit techniques that could be used to intentionally disable DeviceLock Service. When this protection is turned on, the DeviceLock Driver controls the integrity of its code. If a violation is found, DeviceLock causes Windows to stop with a fatal error (BSOD).

Note: Some antivirus, firewall and other low-level third-party software may conflict with the unhook protection and cause fatal errors (BSOD). We recommend that you enable this protection only for the systems where it was tested before.

If you select the **Log Only** check box, DeviceLock does not cause Windows to stop with a fatal error (BSOD) when a violation is found. Instead, the event about this violation is written into the audit log.

Select the **Prevent Changes In System Configuration Files** check box to instruct DeviceLock Service to automatically secure the Windows Hosts file.

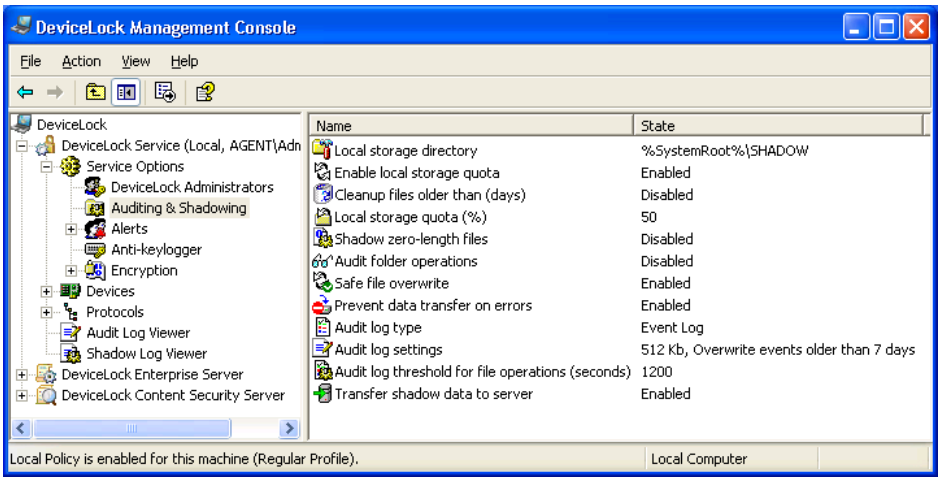
Note: Because DeviceLock uses the local Hosts file for host name resolution, a malicious user with local administrator rights can modify the Hosts file as required to bypass DeviceLock security policies. In order to minimize security risks, we recommend that you secure the Hosts file using the **Prevent Changes In System Configuration Files** option.

Also, by selecting or clearing the **Use Strong Integrity Check** check box, you can specify the type of integrity checks to use. You can run two types of integrity checks to detect corruption in DeviceLock Service's executable files:

- Simple integrity check: DeviceLock Service checks version information of all its executable files. To specify this type of integrity checks, clear the **Use Strong Integrity Check** check box.
- Strong integrity check: DeviceLock Service verifies the digital signatures of all its executable files. To specify this type of integrity checks, select the **Use Strong Integrity Check** check box. A strong integrity check requires more time than a simple integrity check.

Auditing & Shadowing

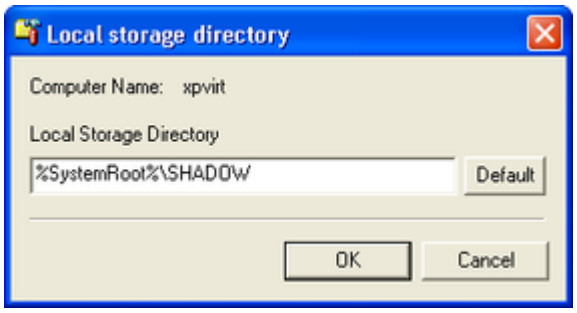
These parameters allow you to tune up auditing and shadowing for DeviceLock Service.



Use the context menu available via a right mouse click on every parameter.

Local storage directory

Use this parameter to define where on the local disk cached data (audit/shadowing data, data for content analysis and the alert queue) is stored.



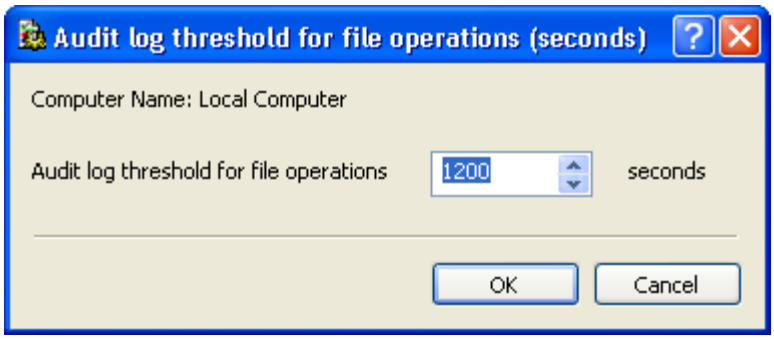
By default, DeviceLock Service uses the ***%SystemRoot%\SHADOW*** directory to store cached data (audit/shadowing data, data for content analysis and the alert queue) on the local computer. %SystemRoot% is a standard environment variable that expands to a path to the Windows root folder (for example, C:\Windows). You can specify any other directory on any locally accessible hard disk.

DeviceLock Service protects this directory so regular users cannot access files inside it.

Make sure that there is enough space to store the data (if the user copies 1GB to the flash drive, then you need approximately 2GB available in local storage).

Audit log threshold for file operations (seconds)

You can specify the time threshold, in seconds, used for consolidation of repetitive events associated with file operations.



The default is 1200 seconds. After this amount of time passes without new repetitive events being recorded, multiple repetitive events are combined into a single summary event if all of the following conditions are true:

- The events are associated with the same user
- The events are associated with the same process
- The events are associated with the same file operation (such as read, write, etc.) on a file.

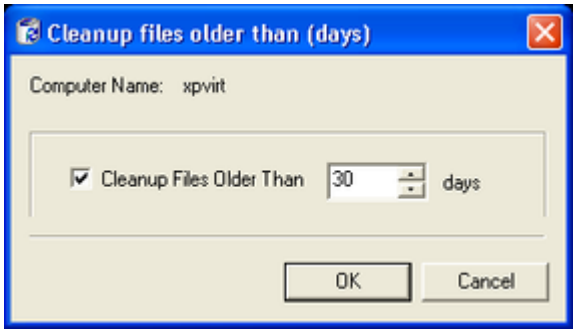
Enable local storage quota

Enable this parameter to allow automatic cleanup of the locally stored cached data (for shadowing and content analysis).

When this parameter is enabled you can also configure **Cleanup files older than (days)** and **Local storage quota (%)** parameters (see below).

Cleanup files older than (days)

You can define the number of days that should pass before cached data (for shadowing and content analysis) can be automatically deleted from the local storage.



Select the **Cleanup Files Older Than** check box and type or select the number of days to allow automatic cleanup.

Local storage quota (%)

You can define a disk quota for cached data (audit/shadowing data, data for content analysis and the alert queue).

Specify the maximum percentage (from 5 to 100) of free disk space that can be used by cached data in the **Local Storage Quota** parameter.

If the quota is not used (i.e. the **Enable local storage quota** parameter is disabled) then DeviceLock Service uses all available space on the disk where the directory specified in the **Local storage directory** parameter is located.

When the total size of the directory specified in the **Local storage directory** parameter reaches the quota, DeviceLock Service either starts deleting old data (if the **Cleanup files older than (days)** parameter is enabled) or stops data shadowing and content analysis (if the **Cleanup files older than (days)** parameter is disabled or there is nothing to delete).

Shadow zero-length files

Enable this parameter to allow shadowing of files whose size is zero.

Even if the file contains no data at all, it is still possible to transfer some information in its name and path (up to several kilobytes) that is why you may need to enable shadowing for zero-length files.

Audit folder operations

Enable this parameter to turn on audit logging of events associated with operations on folders, such as creating (writing), renaming, reading (opening), and deleting folders. When this parameter is disabled, all events associated with folder operations will be excluded from auditing.

Safe file overwrite

Enable this parameter to prevent user's original file deletion following write-denied file activities with the same file name. While the changes are not kept due to the content violation, the original file remains in the folder. An audit log event is recorded when the original file is restored.

Prevent data transfer on errors

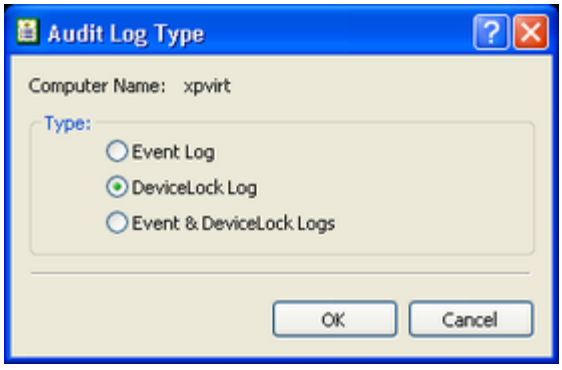
By enabling this parameter, you can prevent users from writing data when shadowing or content analysis is not possible.

You can be sure that users can transfer information only when shadowing and Content-Aware Rules are working normally (e.g. there is enough local disk space to store cached data).

When the **Prevent data transfer on errors** parameter is enabled, the total size of the directory specified in the **Local storage directory** parameter reaches the quota specified in **Local storage quota (%)** and there is no data that can be deleted, DeviceLock Service stops shadowing and content analysis and blocks any user attempt to copy the data.

Audit log type

Using this parameter you can define what log should be used to store audit records.



There are three options to choose:

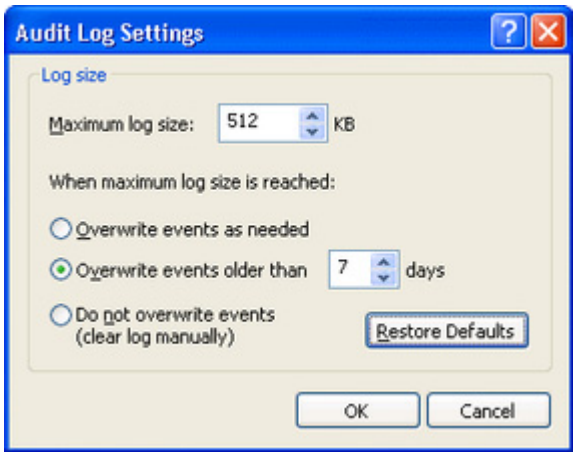
- **Event Log** – only the standard local Windows Event Log is used to store audit records.

- **DeviceLock Log** – only the protected proprietary log is used to store audit records. The data from this log is sent to DeviceLock Enterprise Server and is stored centrally in the database.
- **Event & DeviceLock Logs** – both logs are used to store audit records.

Audit log settings

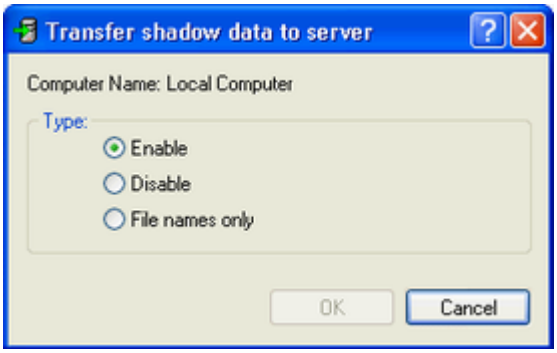
Use **Audit log settings** to specify the maximum size of the audit log and overwrite options.

For a detailed description of the audit log settings, see "Audit Log Settings (Service)."



Transfer shadow data to server

Use this parameter to set options for transfer of shadow data to DeviceLock Enterprise Server.



There are three options to choose:

- **Enable** – all shadow data is transferred to DeviceLock Enterprise Server.
- **Disable** - only audit data from the DeviceLock proprietary log (if this log is used) is sent to DeviceLock Enterprise Server, while all shadow data is stored locally and is not transferred to the server.
- **File names only** – only shadow file names, but not shadow files themselves are transferred to DeviceLock Enterprise Server. Shadow files are stored locally on client computers and can be transferred later to DeviceLock Enterprise Server if you select the **Enable** option for the **Transfer shadow data to server** parameter.

Note: By default, if shadow files are first transferred to DeviceLock Enterprise Server in "File names only" mode and then removed to the Deleted Shadow Data Log and after that you select the **Enable** option for the **Transfer shadow data to server** parameter, the following behavior occurs: These shadow files will not be transferred to DeviceLock Enterprise Server and will be deleted locally on client computers.

Alerts

You can define alerts to automatically notify you of significant incidents, events or problems when they occur. Real-time alerting simplifies event monitoring and log management and helps you response faster and more efficiently to security incidents and policy violations.

DeviceLock supports the following types of alerts:

- Alerts that are generated when a specific user attempts to access a specific device type or a protocol.
- Alerts that are generated when a specific Content-Aware Rule fires.
- Alerts that are generated when a specific firewall rule fires.
- Administrative alerts. Some examples of administrative alerts include "Notify if Service settings are changed"; "Notify if Service settings are corrupted" and many others.

Alerts can be sent to their intended recipients through e-mail or SNMP traps.

Before DeviceLock can send alert notifications, you should do the following:

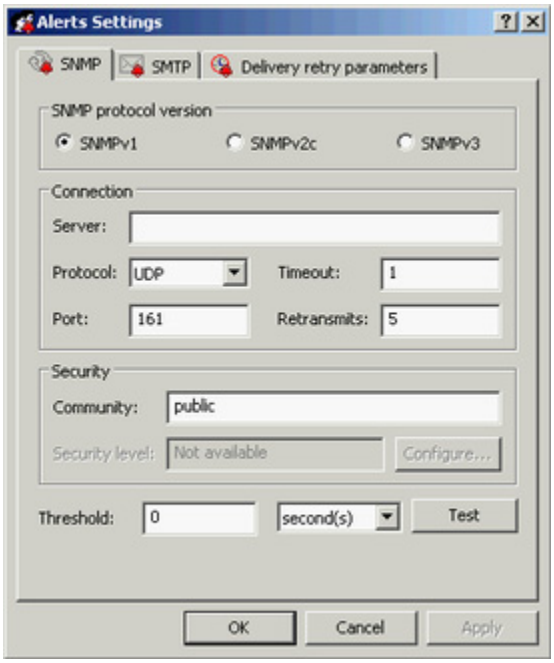
- Decide how you want to be notified when alert conditions occur: through SNMP traps or e-mail.
- If you want to be notified through SNMP traps, configure DeviceLock Service for SNMP support and specify the SNMP server to send traps to.

  Note: This manual assumes a basic understanding of the Simple Network Management Protocol (SNMP) and related network management concepts.

- If you want to be notified through e-mail, configure e-mail notifications by specifying SMTP Server and e-mail notification settings and defining the e-mail templates.
- Configure alert delivery failure parameters such as the delivery retry count, delivery retry interval, and the amount of time an undelivered notification is kept in the queue for delivery.
- Enable notifications for specific events. When you enable notifications for specific events, you specify the conditions for which you want to be notified. For information on how to enable administrative alerts, see "Administrative Alerts." For information on how to enable device type-specific alerts, see "Auditing, Shadowing & Alerts (Regular Profile)". For information on how to enable protocol-specific alerts, see "Managing Audit, Shadowing and Alerts for Protocols." For information on how to enable alerts for a specific Content-Aware Rule, see "Defining Content-Aware Rules" (for devices) and "Defining Content-Aware Rules" (for protocols). For information on how to enable alerts for a specific firewall rule, see "Managing Basic IP Firewall" and "Defining Firewall Rules."

Alerts Settings Dialog Box: SNMP Tab

Use the **SNMP** tab in the **Alerts Settings** dialog box to configure DeviceLock Service for SNMP support.



This dialog box appears in one of the following situations:

- When you right-click **Alerts** in the console tree, and then click **Manage**.
- When you select **Alerts** in the console tree, and then click **Manage** on the toolbar.
- When you select **Alerts** in the console tree, and then in the details pane, right-click **SNMP**, and click **Manage**.
- When you select **Alerts** in the console tree, and then in the details pane, double-click **SNMP**.

Note: You can define different online vs. offline alert settings. Online alert settings (Regular Profile) apply to client computers that are working online. Offline alert settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)."

DeviceLock supports SNMPv1, SNMPv2c, and SNMPv3 protocols. You can configure DeviceLock Service to automatically send alert notifications to the specified SNMP server when alert conditions occur. These alerts are sent only when all of the following conditions are met:

- The SNMP server is set up to receive traps.
- The remote computer running the SNMP server is accessible from all computers running DeviceLock Service.
- Alerts have been configured to be sent through SNMP traps.

In the **Alerts Settings** dialog box, on the **SNMP** tab, do the following:

USE THIS	TO DO THIS
SNMP protocol version	Configure DeviceLock Service to use the version of SNMP supported by the SNMP server. Available options are: **SNMPv1**, **SNMPv2c**, and **SNMPv3**.
Connection	Configure the SNMP server information.
Server	Specify the SNMP sever to send traps to. To do so, in the **Server:** box, type the SNMP server host name or IP address.
Protocol	Specify the transport protocol for passing data between DeviceLock Service and the SNMP server. Available options are: **UDP** and **TCP**.
Timeout	Specify the time (in seconds) that DeviceLock Service waits for the SNMP server to reply before retransmitting the data packet. The default is **1** second.
Port	Specify the port on which the SNMP server listens for traps. The default is **161**.
Retransmits	Specify the number of times DeviceLock Service's request is re-sent to the

USE THIS	TO DO THIS
	SNMP server, if the server is not responding. The default is **5**. *This value is set only for TCP connections*.
Security	Configure SNMP security settings.
Community	Specify the SNMP community string to use for authentication with the SNMP server. The default is **public**. Applicable only to SNMP v1 and SNMPv2c.
Security user name	Specify the user account to use for authentication with the SNMP server. Applicable only to SNMP v3. If authentication is not required, no authentication credentials need to be specified.
Context name	Specify the context name if an SNMP context is configured on the SNMP server. Applicable only to SNMP v3.
Context Engine ID	Specify the context engine ID if an SNMP context is configured on the SNMP server. Applicable only to SNMP v3.
Authentication protocol	Specify the protocol used to encrypt the authentication with the SNMP server. Applicable only to SNMP v3. Available options: **None** (corresponds to the SNMP security level "**No security**" – communication without authentication and without privacy), **HMAC-MD5** (corresponds to the SNMP security level "**Authentication**"); **HMAC-SHA** (corresponds to the SNMP security level "**Authentication**").
Password/ Confirm password	Specify the password corresponding to the user account to use for authentication with the SNMP server. Applicable only to SNMP v3.
Privacy protocol	Specify the protocol used to encrypt data for SNMP communication. Applicable only to SNMP v3. Available options: **None** (corresponds to the SNMP security level "**Authentication**" - communication with authentication and without privacy), **CBC-DES** (corresponds to the SNMP security level "**Authentication and Privacy**" - communication with authentication and privacy); **CBC-AES-28** (corresponds to the SNMP security level "**Authentication and Privacy**" - communication with authentication and privacy).
Password/ Confirm password	Specify the password for data encryption (privacy). Applicable only to SNMP v3.
Threshold	Specify the time interval (in hours, minutes and seconds) used for event consolidation when generating alerts. DeviceLock Service consolidates multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true: 1. The events are of the same type, either **Success** for allowed access or **Failure** for denied access. 2. The events are associated with the same device type/protocol. 3. The events are associated with the same user. 4. The events are associated with the same PID. The default is **0** seconds.

USE THIS	TO DO THIS
	Note: DeviceLock Service combines only access-related events when generating alerts. Administrative events are not consolidated.
Test	Send a test SNMP trap to verify that DeviceLock Service is configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed: 1. The test can complete successfully, meaning that a test SNMP trap was successfully sent using the configured SNMP trap parameters. The resulting message states: "Test SNMP alert was successfully sent." 2. The test can fail, meaning that a test SNMP trap was not sent. The resulting message states: "Test SNMP alert was not sent due to error: *<error_description>*."

SNMP traps generated by DeviceLock Service are sent in the Management Information Base (MIB) format. The private DeviceLock MIB is represented by the object identifier (OID) **1.3.6.1.4.1.60000** or **iso.org.dod.internet.private.enterprise.DeviceLock**. The DeviceLock MIB contains the following branch nodes:

- **products(1)**
- **agent(1)**
- **alerts(1)** This node contains the following single MIB objects:
  - **eventType(1)** – the class of an event: **Success** for allowed access, **Failure** for denied access, or **Information** for events generated by Content-Aware rules of "Detection" type. Please note that the value of **eventType** is displayed as a numeric value instead of a text string: "**8**" indicates success, "**16**" indicates failure, and "**4**" indicates information.
  - **eventId(2)** – a number identifying the particular event type.
  - **userSid(3)** – the security identifier (SID) of the user associated with this event.
  - **userName(4)** – the name of the user associated with this event.
  - **computerName(5)** – the name of the computer from which the event was received.
  - **processId(6)** – the identifier of the process associated with this event.
  - **processName(7)** – the name of the process associated with this event.
  - **source(8)** – the type of device or protocol involved. Please note that the value of **source** is displayed as a numeric value instead of a text string. The following numeric values are used:

"1" indicates "Floppy" "2" indicates "Removable" "3" indicates "Hard disk" "5" indicates "Optical Drive" "7" indicates "Serial port" "8" indicates "Parallel port" "9" indicates "Tape" "10" indicates "USB port" "11" indicates "Infrared port" "12" indicates "FireWire port" "13" indicates "Bluetooth" "14" indicates "WiFi" "15" indicates "Windows Mobile" "16" indicates "Palm" "17" indicates "Printer" "18" indicates "iPhone" "19" indicates "BlackBerry" "20" indicates "Clipboard" "21" indicates "TS Devices" "22" indicates "MTP"	"513" indicates "ICQ/AOL Messenger" "514" indicates "HTTP" "515" indicates "Torrent" "516" indicates "FTP" "517" indicates "SMTP" "518" indicates "Windows Messenger" "519" indicates "Yahoo Messenger" "520" indicates "Jabber" "521" indicates "IRC" "522" indicates "Telnet" "524" indicates "Mail.ru Agent" "525" indicates "Web Mail" "526" indicates "Social Networks" "527" indicates "SSL" "528" indicates "SMB" "529" indicates "MAPI" "530" indicates "File Sharing" "531" indicates "Skype" "533" indicates "Any (TCP)" "534" indicates "Any (UDP)" "539" indicates "IP (TCP)" "540" indicates "IP (UDP)" "541" indicates "IBM Notes" "542" indicates "WhatsApp Web"

- **action(9)** – the user's activity type.
- **name(10)** – the name of the object (file, USB device, etc.).
- **info(11)** – other device-specific information for the event, such as the access flags, device names, and so on.
- **reason(12)** – the cause of the event.
- **datetime(13)** – the date and time (in the RFC3339 date/time format) when the event was received by DeviceLock Service.

Note: These MIB objects correspond to audit log fields.

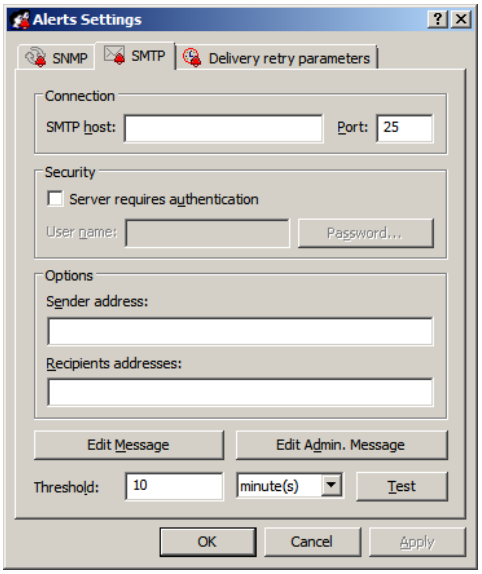
A trap is sent just once each time an event associated with an alert occurs.

Below is an example of an SNMP alert.

- Specific: 1
  - Message reception date: 12.09.2012
  - Message reception time: 12:55:27.466
  - Time stamp: 244 days 08h:34m:52s.24th
  - Message type: Trap (v1)
  - Protocol version: SNMPv1
  - Transport: IP/UDP
  - Agent
    - Address: 10.10.30.15
    - Port: 62562
  - Manager
    - Address: 10.10.30.16
    - Port: 0
  - Community: public
  - SNMPv1 agent address: 10.10.30.15
  - Enterprise: enterprises.60000
  - Bindings (13)
    - Binding #1: enterprises.60000.1.1.1.1 *** (gauge) 16
    - Binding #2: enterprises.60000.1.1.1.2 *** (gauge) 13
    - Binding #3: enterprises.60000.1.1.1.3 *** (octet string) S-1-5-21-3601177953-2830843172-1403898981-500
    - Binding #4: enterprises.60000.1.1.1.4 *** (octet string) Win7x64\Administrator
    - Binding #5: enterprises.60000.1.1.1.5 *** (octet string) WIN7X64
    - Binding #6: enterprises.60000.1.1.1.6 *** (gauge) 456
    - Binding #7: enterprises.60000.1.1.1.7 *** (octet string) C:\Windows\Explorer.EXE
    - Binding #8: enterprises.60000.1.1.1.8 *** (gauge) 2
    - Binding #9: enterprises.60000.1.1.1.9 *** (octet string) Write
    - Binding #10: enterprises.60000.1.1.1.10 *** (octet string) E:\Market research.docx
    - Binding #11: enterprises.60000.1.1.1.11 *** (octet string) (zero-length)
    - Binding #12: enterprises.60000.1.1.1.12 *** (octet string) Rule: "Confidential data" (Any keyword matched)
    - Binding #13: enterprises.60000.1.1.1.13 *** (octet string) 2012-09-12T08:55:26Z

Alerts Settings Dialog Box: SMTP Tab

Use the **SMTP** tab in the **Alerts Settings** dialog box to configure e-mail notifications.



This dialog box appears in one of the following situations:

- When you right-click **Alerts** in the console tree, and then click **Manage**.
- When you select **Alerts** in the console tree, and then click **Manage** on the toolbar.
- When you select **Alerts** in the console tree, and then in the details pane, right-click **SMTP**, and click **Manage**.
- When you select **Alerts** in the console tree, and then in the details pane, double-click **SMTP**.

Note: You can define different online vs. offline alert settings. Online alert settings (Regular Profile) apply to client computers that are working online. Offline alert settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)."

DeviceLock uses the Simple Mail Transfer Protocol (SMTP) for e-mail messaging. You can configure DeviceLock Service to automatically send notifications to the specified e-mail address(es) when alert conditions occur. To configure e-mail notifications, you must do the following:

- Specify SMTP server and e-mail notification settings.
- Define the e-mail templates.

DeviceLock comes with ready-to-use e-mail message templates that you can use to define the message content. These templates determine the basic content, format, and structure of e-mail notifications. DeviceLock provides the following templates:

- An e-mail message for administrative alerts.
- An e-mail message for all other alerts.

Each e-mail template contains the following information:

- **Message subject** – The text used in the **Subject** line of the e-mail message. By default, the subject text of the e-mail message for administrative alerts is as follows: **DeviceLock Administrative Alert**. By default, the subject text of the e-mail message for all other alerts is as follows: **DeviceLock Alert**.
- **Message body** – The text used in the body of the e-mail message. DeviceLock can send either the plain text body or an HTML version of the message body. The message body is the same in both templates and includes static text and macros. By default, the static text in the message body is as follows: **The following event has occurred:**. You can use the following predefined macros in the **Subject** line and/or the body of the e-mail message:
  - **%EVENT_TYPE%** – inserts the class of an event: either **Success** for allowed access or **Failure** for denied access.
  - **%COMP_NAME%** – inserts the name of the computer from which the event was received.
  - **%COMP_IP%** – inserts the comma-delimited list of all network addresses (IPs) associated with the computer.

- **%DATE_TIME%** – inserts the date and time when the event was received by DeviceLock Service. The date and time are displayed based on the client computer's regional and language settings.
- **%SOURCE%** – inserts the type of device or protocol involved.
- **%ACTION%** – inserts the user's activity type.
- **%NAME%** – inserts the name of the object (file, USB device, etc.).
- **%INFO%** – inserts the other device-specific information for the event, such as the access flags, device names, and so on.
- **%REASON%** – inserts the cause of the event.
- **%USER_NAME%** – inserts the name of the user associated with this event.
- **%USER_SID%** – inserts the security identifier (SID) of the user associated with this event.
- **%PROC_NAME%** – inserts the name of the process associated with this event.
- **%PROC_ID%** – inserts the identifier of the process associated with this event.
- **%EVENT_ID%** – inserts a number identifying the particular event type.
- **%SUMMARY_TABLE%** - inserts a table detailing and visualizing individual events for consolidated alerts.

These macros are replaced with their actual values at the message generation time.

In the **Alerts Settings** dialog box, on the **SMTP** tab, do the following:

USE THIS	TO DO THIS
Connection	Configure the e-mail server connection information for notification e-mails.
SMTP host	Specify the SMTP server host name or IP address.
Port	Specify the port number through which e-mail is sent to your e-mail server. The default is **25**. **Note:** Both non-SSL (unencrypted) and SSL connections to the specified SMTP server are supported. DeviceLock automatically identifies encrypted connections and their type.
Security	Set the SMTP security options.
Server requires authentication	Specify the type of authentication to use with the SMTP server. Select the **Server requires authentication** check box to specify basic authentication. Clear the **Server requires authentication** check box to specify no authentication.
User name	Specify the user name to use for authentication with the SMTP server. This property requires a value if you specified basic authentication.
Password/ Confirm password	Specify the password to use for authentication with the SMTP server. This property requires a value if you specified basic authentication.
Options	Define the e-mail sender and recipients.

USE THIS	TO DO THIS
Sender address	Specify the e-mail address from which the alerts will be sent.
Recipients addresses	Specify the e-mail addresses of e-mail recipients (those who will receive the e-mail notification of events). Multiple e-mail addresses must be separated by a comma (,) or semicolon (;).
Edit Message	Customize the predefined contents of the e-mail message for alerts based on the template. In the **E-mail Message for Alerts** dialog box that opens you can also do the following: 1. Change the message format for all messages to HTML or plain text. To do so, click either **Text** or **HTML**. By default, e-mail messages are sent in plain text format. 2. Load the specified message body from a tab-delimited text file (.txt). To do so, click **Load**. The entire contents of the file are loaded. The text can be either plain text or HTML as needed. 3. Restore the default settings. To do so, click **Restore Defaults**.
Edit Admin. Message	Customize the predefined contents of the e-mail message for administrative alerts based on the template. In the **E-mail Message for Administrative Alerts** dialog box that opens you can also do the following: 1. Change the message format for all messages to HTML or plain text. To do so, click either **Text** or **HTML**. By default, e-mail messages are sent in plain text format. 2. Load the specified message body from a tab-delimited text file (.txt). To do so, click **Load**. The entire contents of the file are loaded. The text can be either plain text or HTML as needed. 3. Restore the default settings. To do so, click **Restore Defaults**.
Threshold	Specify the time interval (in hours, minutes and seconds) used for event consolidation when generating alerts. DeviceLock Service consolidates multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true: 1. The events are of the same type, either **Success** for allowed access or **Failure** for denied access. 2. The events are associated with the same device type/protocol. 3. The events are associated with the same user. 4. The events are associated with the same PID. The default is **10** minutes. **Note:** DeviceLock Service combines only access-related events when generating alerts. Administrative events are not consolidated.
Test	Send a test e-mail notification to verify that DeviceLock Service is

USE THIS	TO DO THIS
	configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed: 1. The test can complete successfully, meaning that a test e-mail notification was successfully sent using the configured e-mail notification parameters. The resulting message states: "Test SMTP alert was successfully sent." 2. The test can fail, meaning that a test e-mail notification was not sent. The resulting message states: "Test SMTP alert was not sent due to error: *<error_description>*."

Below is an example of an e-mail alert.

DeviceLock Alert

The following event has occurred:
Event type: Failure (16)
Computer: WIN7X64
Date/Time: 09/11/12 18:24:38
Source: Removable (2)
Action: Write
Name: E:\Market research.docx
Info:
Reason: Rule: "Confidential data" (Any keyword matched)
User name: Win7x64\Administrator
User SID: S-1-5-21-3601177953-2830843172-1403898981-500
Process name: C:\Windows\Explorer.EXE
Process Id: 456
Event id: 13

Note: Field names in an e-mail alert correspond to field names in the Audit Log.

Alerts Settings Dialog Box: Delivery retry parameters Tab

Use the **Delivery retry parameters** tab in the **Alerts Settings** dialog box to configure alert delivery failure parameters.

This dialog box appears in one of the following situations:

- When you right-click **Alerts** in the console tree, and then click **Manage**.
- When you select **Alerts** in the console tree, and then click **Manage** on the toolbar.
- When you select **Alerts** in the console tree, and then in the details pane, right-click **Delivery retry parameters**, and click **Manage**.
- When you select **Alerts** in the console tree, and then in the details pane, double-click **Delivery retry parameters**.

Note: You can define different online vs. offline alert settings. Online alert settings (Regular Profile) apply to client computers that are working online. Offline alert settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)."

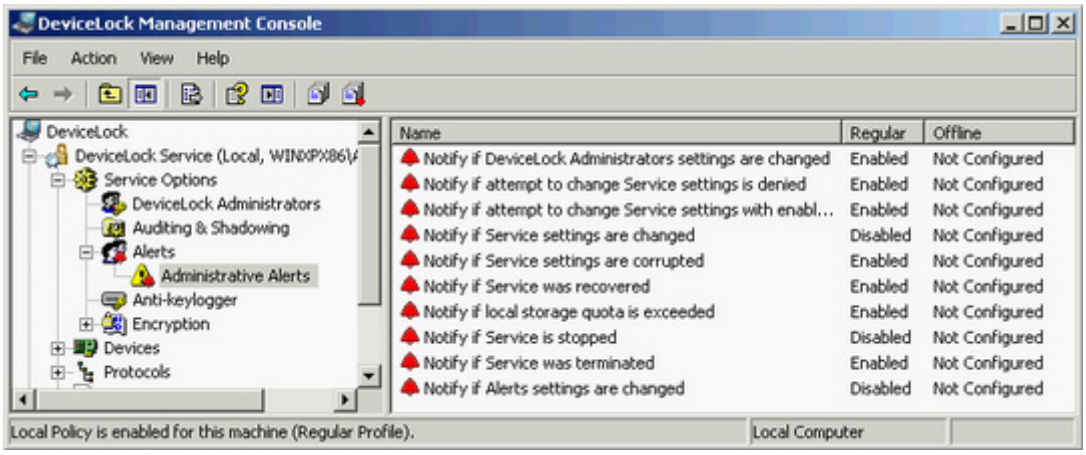
DeviceLock generates and delivers alerts the moment the alert conditions are met. If alerts cannot be delivered on the first try, DeviceLock creates a queue to store undelivered alerts for a specified amount of time and sends them again. You can specify the maximum number of times DeviceLock attempts to send an alert, set the interval between delivery tries and also define the amount of time undelivered alerts are kept in the queue for delivery.

In the **Alerts Settings** dialog box, on the **Delivery retry parameters** tab, do the following:

USE THIS	TO DO THIS
Delivery retry count	Specify the maximum number of times DeviceLock attempts to send an alert if the first delivery attempt fails. If the first delivery attempt fails, the alert is deferred to the queue and marked as having had one delivery attempt. Thereafter, each time the queued alert is sent and delivery fails, the number of attempts is incremented. This parameter must contain a value between 0 and 999. The default value is **3** retries. When the delivery retry count is reached and delivery fails, DeviceLock logs an error in the Audit Log ("%*Channel_name*% for alerts is unavailable and temporary disabled due to error: %*error_code*% - %*error_description*%") and temporarily stops further transmissions through the alert delivery channel (SNMP and/or SMTP). DeviceLock will automatically attempt to re-establish connection with the specified SNMP or SMTP server when checking its connection state (whether it is online or offline). If the connection is restored, DeviceLock resumes sending alerts. Different values of this parameter are used for regular and offline profiles.
Delivery retry interval: seconds	Specify how many seconds DeviceLock waits before it attempts next delivery of the alert, if the previous delivery failed. This parameter must contain a value between 10 and 3600.The default value is **600** seconds.
Keep in queue: hours	Define the amount of time in hours undelivered alerts are kept in the queue for delivery before they are deleted. The same queue is used for all delivery channels (SNMP and/or SMTP). This parameter must contain a value between 1 and 999. The default value is **1** hour. This parameter can be specified only for the regular profile. The same value of this parameter is used for both profiles (regular and offline).

Administrative Alerts

You can enable administrative alerts to automatically notify you of critical events, requiring direct administrator actions. Once enabled, an alert will be sent to the specified destinations when such a critical event is encountered.



Available administrative alerts include:

- **Notify if DeviceLock Administrators settings are changed** – DeviceLock sends this notification when any changes have been made to the DeviceLock Administrators settings. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.
- **Notify if attempt to change Service settings is denied** – DeviceLock sends this notification when DeviceLock Security is enabled and a user with insufficient access rights attempts to modify DeviceLock Service settings multiple times over a short period. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.
- **Notify if attempt to change Service settings with enabled "Override Local Policy" is denied** – DeviceLock sends this notification when the **Override Local Policy** parameter is enabled in DeviceLock Group Policy Manager and any user that connected DeviceLock Management Console to the computer running DeviceLock Service attempts to modify the service's settings. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.
- **Notify if Service settings are changed** – DeviceLock sends this notification when one or more DeviceLock Service settings (except for DeviceLock Administrators settings) have been modified. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the type of device or protocol involved, the user's activity type, the type of the profile, the name of the user, the user's SID, and the event ID.
- **Notify if Service settings are corrupted** – DeviceLock sends this notification when DeviceLock Service starts and detects corruption of its settings. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.

DeviceLock Service uses a checksum calculation to validate its settings.

All corrupted settings are automatically restored.

- **Notify if Service was recovered** – DeviceLock sends this notification when the DeviceLock Driver starts and detects removal of one or more DeviceLock Service installation files. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.
  All missing files are automatically restored.
- **Notify if local storage quota is exceeded** – DeviceLock sends this notification when the local storage quota for audit/shadowing data, the alert queue, and data for content analysis has been exceeded. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.
  For detailed information on the local storage quota, see "Local storage quota."
- **Notify if Service is stopped** – DeviceLock sends this notification when DeviceLock Service starts after it has been stopped. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the version number of DeviceLock Service, the name of the user, the user's SID, and the event ID.
- **Notify if Service is uninstalled** – DeviceLock sends this notification when DeviceLock Service is uninstalling. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the version number of DeviceLock Service, the name of the user, the user's SID, and the event ID.
- **Notify if Service was terminated** – DeviceLock sends this notification when DeviceLock Service restarts after incorrect termination. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the version number of DeviceLock Service, the name of the user, the user's SID, and the event ID.
- **Notify if Alerts settings are changed** – DeviceLock sends this notification when one or more alert settings have been modified. The notification is sent according to the previous alert settings. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the type of the profile, the name of the user, the user's SID, the identifier of the process associated with this event, and the event ID.
- **Notify if keylogger is detected** – DeviceLock sends this notification when hardware USB keylogger is detected. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the USB device detected as a keylogger, the name of the user, the user's SID, and the event ID. The **Log event** parameter in **Anti-keylogger** options should be enabled to allow this notification. For more information, please read the Anti-keylogger section of this manual.

Administrative alerts can be enabled individually or collectively.

Note: You can enable different online vs. offline administrative alerts. Online alerts (Regular Profile) are generated when client computers are working online. Offline alerts (Offline Profile) are generated when client computers are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)."

To enable online (regular) or offline administrative alerts individually, right-click any Administrative Alert, and then click **Enable** or **Enable Offline**. The Administrative Alert changes its online/offline state from "Not Configured" to "Enabled."

Once you have enabled a particular Administrative Alert, you can disable it. To do so, right-click the enabled Administrative Alert, and then click **Disable** or **Disable Offline**. The Administrative Alert changes its state from "Enabled" to "Disabled".

You can also disable or enable an online (regular) alert by double-clicking it.

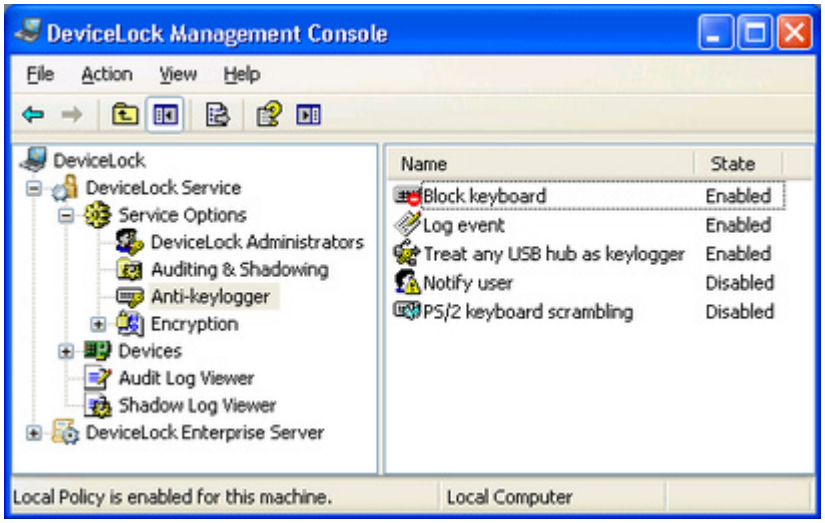
To enable online (regular) or offline administrative alerts collectively, right-click any Administrative Alert, and then click **Manage** or **Manage Offline**. Alternatively, you can select any Administrative Alert, and then click **Manage** or **Manage Offline** on the toolbar. Next, in the dialog box that opens, select the appropriate check boxes for the administrative alerts that you want to enable. Once you have enabled Administrative alerts, you can disable them. To do so, clear the appropriate check boxes.

Note: All check boxes in the **Administrative alerts (Offline)** dialog box have three states: selected, cleared, and indeterminate that correspond to the Enabled, Disabled, and Not Configured states of administrative alerts.

Anti-keylogger

These parameters allow you to tune up DeviceLock's ability to detect hardware keyloggers and to define what DeviceLock Service should do when a keylogger is found.

Hardware keyloggers are devices that record keystrokes. DeviceLock Service can detect USB keyloggers and block keyboards connected to them. Also, DeviceLock Service can block PS/2 keyloggers.



Use the context menu available via a right mouse click on every parameter.

Block keyboard

Enable this parameter to block the keyboard connected to the hardware USB keylogger when it is detected.

Since DeviceLock Service starts before the user logs in to Windows, it can block the keyboard and prevent the user from typing the password.

Note: Some hardware keyloggers continue to record keystrokes even if the keyboard is blocked and not functioning in Windows. This happens because such keyloggers are standalone devices and do not require any OS or drivers.

Log event

You can instruct DeviceLock Service to write an event to the audit log when the hardware USB keylogger is detected.

Treat any USB hub as keylogger

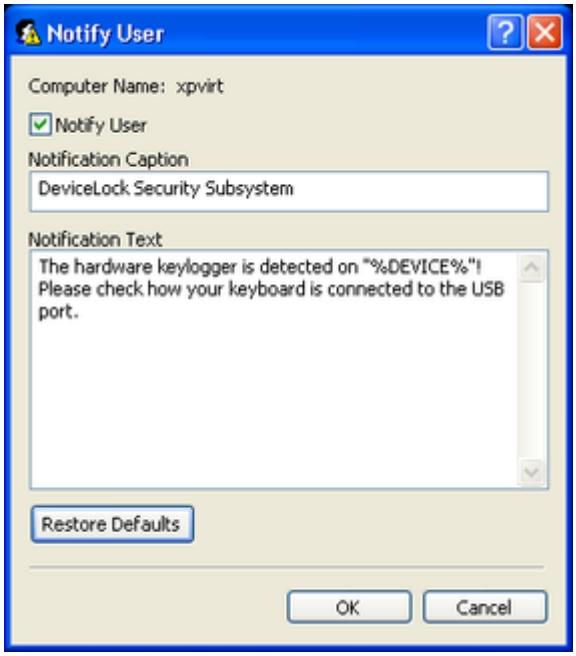
By enabling this parameter, you can instruct DeviceLock Service to treat any external USB hub to which the keyboard is connected as a hardware keylogger.

Otherwise, DeviceLock Service detects only those hub keyloggers that exist in its internal database.

Notify user

You can define a custom message to be displayed to users when DeviceLock Service detects hardware USB keyloggers.

Since DeviceLock Service starts before the user logs in to Windows, this message can alert the user and prevent him/her from typing the password on the keyboard connected to the USB keylogger.



To enable this custom message, select the **Notify User** check box.

Also, you can define additional parameters, such as:

- **Notification Caption** – the text to be displayed as a caption. You can use the predefined macros within the text: **%DEVICE%** – inserts the name of the keyboard's device (for example, USB Keyboard) received from the system.
- **Notification Text** – the main text of the message. You can use the predefined macros described above within the text.

PS/2 keyboard scrambling

By enabling this parameter, you can prevent PS/2 keyloggers from recording keystrokes. DeviceLock Service is unable to detect PS/2 keyloggers and notify users about their presence but it obfuscates PS/2 keyboard's input and forces PS/2 keyloggers (if any) to record some garbage instead of the real keystrokes.

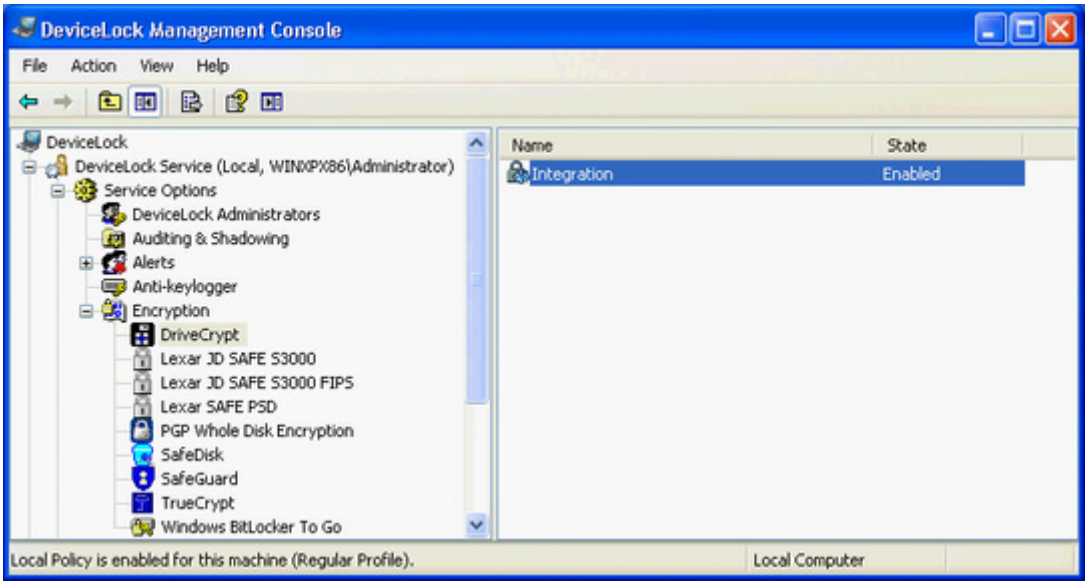
Note: When PS/2 keyboard scrambling is enabled while working with the PS/2 KVM switch, the switching between computers will not work from the keyboard.

Encryption

DeviceLock Service can detect disks (USB flash drives and other removable media) encrypted by third-party products and apply special "encrypted" permissions to them.

This feature allows you to define more flexible access control policies and helps to prevent writing sensitive data to unencrypted media.

Currently DeviceLock supports these third-party products for encrypting data on removable storage devices:



- **DriveCrypt** – DeviceLock Service can detect DriveCrypt Plus Pack's (DCPP) encrypted removable storage devices and apply special "encrypted" permissions to them when the DriveCrypt Plus Pack product is installed on the computer where DeviceLock Service is running and **Integration** is enabled. For more information on DriveCrypt Plus Pack, please visit: http://www.securstar.com
- **Lexar JD SAFE S3000** and **Lexar JD SAFE S3000 FIPS** – DeviceLock Service can detect Lexar™ JumpDrive SAFE S3000 USB flash drives (FIPS-certified and/or regular) and apply special "encrypted" permissions to them in the event that a user plugs such a device into a computer where DeviceLock Service is running and **Integration** is enabled. For more information on Lexar™ JumpDrive SAFE S3000, please visit Lexar's Web site: http://www.lexar.com/products/enterprise-usb-solutions.
- **Lexar SAFE PSD** – DeviceLock Service can detect Lexar™ SAFE PSD S1100 USB flash drives and apply special "encrypted" permissions to them in the event that a user plugs such a device into a computer where DeviceLock Service is running and **Integration** is enabled. For more information on Lexar™ SAFE PSD S1100, please visit Lexar's Web site: http://www.lexar.com/about/newsroom/press-releases/lexar-begins-shipping-its-award-winning-safe-psd-s1100-secure-enterpri.

- **PGP Whole Disk Encryption** – DeviceLock Service can detect PGP-encrypted removable storage devices and apply special "encrypted" permissions to them when the PGP® Whole Disk Encryption product is installed on the computer where DeviceLock Service is running and **Integration** is enabled. For step-by-step instructions on how to install and use PGP® Whole Disk Encryption with DeviceLock, please refer to the PGP/DeviceLock Integration Guide created by PGP. For more information on PGP® Whole Disk Encryption, please visit PGP's Web site: http://www.pgp.com/products/wholediskencryption/index.html.
- **SafeDisk** – DeviceLock Service can detect encrypted SafeDisk containers (stored on USB flash drives and other removable media) and apply special "encrypted" permissions to them if **Integration** is enabled. Using these "encrypted" permissions you can, for example, allow writing only to encrypted removable devices and deny writing to unencrypted media. For more information on ViPNet Safe Disk, visit the following Web site http://www.infotecs.biz.

  Note: To get access to SafeDisk containers and work with their contents, users should have at least read access to unencrypted Removable devices.

- **SafeGuard** - DeviceLock Service can detect Sophos SafeGuard Easy-encrypted disks (USB flash drives and other removable media) and apply special "encrypted" permissions to them if **Integration** is enabled. Using these "encrypted" permissions you can, for example, allow writing only to encrypted removable devices and deny writing to unencrypted media. For more information on SafeGuard Easy, visit the Sophos Web site.
- **TrueCrypt** – DeviceLock Service can detect TrueCrypt's encrypted removable storage devices and apply special "encrypted" permissions to them when the TrueCrypt product is installed on the computer where DeviceLock Service is running and **Integration** is enabled. For more information on TrueCrypt, please visit TrueCrypt's Web site: http://www.truecrypt.org/.

  Note: If the TrueCrypt's volume type is "**File-hosted (container)**", then to get access to this container and work with its content, the user should have at least read access to unencrypted Removable devices.

- **Windows BitLocker To Go** - DeviceLock Service can detect BitLocker To Go-encrypted drives and apply special "encrypted" permissions to them if **Integration** is enabled. For more information on the BitLocker Drive Encryption feature of Windows 7 (and later), refer to the Microsoft documentation.

  Note: If integration with Windows BitLocker To Go is enabled, the **Deny write access to removable drives not protected by BitLocker** policy setting (located in **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives**) cannot be enabled.

- **Mac OS X FileVault** - DeviceLock Service for Mac can detect FileVault-encrypted disks (external drives) and apply special "encrypted" permissions to them if **Integration** is enabled. Using these "encrypted" permissions you can, for example, allow writing only to encrypted devices and deny writing to unencrypted drives. For more information on FileVault, visit the Apple Web site.

If you do not want to allow DeviceLock Service to detect one of the encryption products listed above and to apply special "encrypted" permissions to storage devices encrypted by it, disable **Integration** under the product's section in the management console.

For more information on "encrypted" permissions, please read the Permissions section of this manual.

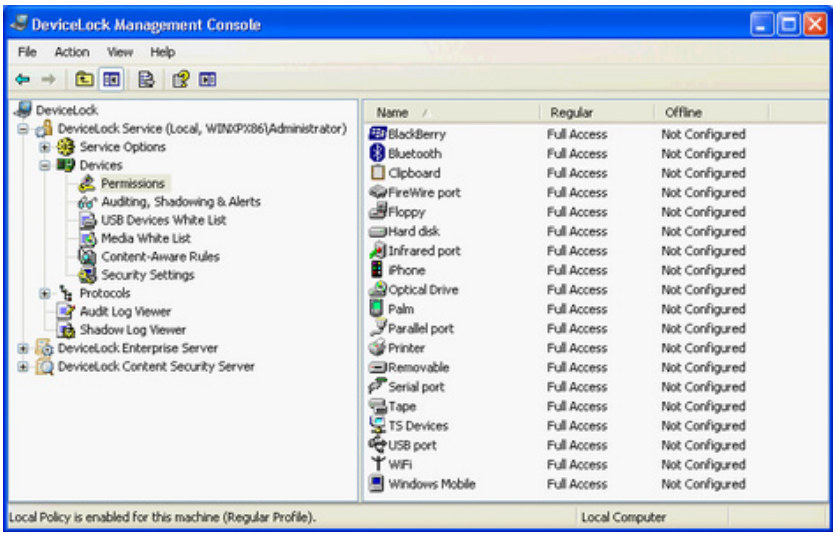
Note: DeviceLock does not ship with third-party encryption products and does not require them for its own functioning. The integrated functioning of DeviceLock and a third-party encryption product will only work when the third-party product is properly installed, configured and running on the same computer where DeviceLock Service is running.

Devices

Configuration parameters available under this item allow you to access main functions of DeviceLock – permissions, auditing, shadowing, white lists and so on.

Permissions (Regular Profile)

There is a list of device types for which you can define user-level permissions.


DeviceLock Management Console
File Action View Help
DeviceLock
DeviceLock Service (Local, WINXPX86\Administrator)
Service Options
Devices
Permissions
Auditing, Shadowing & Alerts
USB Devices White List
Media White List
Content-Aware Rules
Security Settings
Protocols
Audit Log Viewer
Shadow Log Viewer
DeviceLock Enterprise Server
DeviceLock Content Security Server
Name
Regular
Offline
BlackBerry Full Access Not Configured
Bluetooth Full Access Not Configured
Clipboard Full Access Not Configured
FireWire port Full Access Not Configured
Floppy Full Access Not Configured
Hard disk Full Access Not Configured
Infrared port Full Access Not Configured
iPhone Full Access Not Configured
Optical Drive Full Access Not Configured
Palm Full Access Not Configured
Parallel port Full Access Not Configured
Printer Full Access Not Configured
Removable Full Access Not Configured
Serial port Full Access Not Configured
Tape Full Access Not Configured
TS Devices Full Access Not Configured
USB port Full Access Not Configured
WiFi Full Access Not Configured
Windows Mobile Full Access Not Configured
Local Policy is enabled for this machine (Regular Profile).
Local Computer

Note: When you set permissions for a device type, you set these permissions for every device belonging to that type. It is impossible to set different permissions for two different devices if they are of the same type (for example, both are removable drives). To define different permissions for USB devices even if they are of the same type, use the White List function.

There are two levels of control: the interface (port) level and the type level. Some devices are checked at both levels, while others only at the one level – either interface (port) or

type. For more information on how access control works, please read the Managed Access Control section of this manual.

DeviceLock supports the following types of devices:

- **BlackBerry** (type level) – includes all BlackBerry devices with any type of the connection interface (USB, Bluetooth) to the computer.
- **Bluetooth** (type level) – includes all internal and external Bluetooth devices with any type of the connection interface (USB, PCMCIA, etc.) to the computer.
- **Clipboard** – includes the Windows Clipboard. DeviceLock controls copy/paste operations for data placed on the clipboard.
- **FireWire port** (interface level) – includes all devices that can be plugged into the FireWire (IEEE 1394) port, except the hub devices.
- **Floppy** (type level) – includes all internal and external floppy drives with any connection interface (IDE, USB, PCMCIA, etc.). It is possible that some nonstandard floppy drives are recognized by Windows as removable devices, in this case DeviceLock treats such floppy drives as the **Removable** type as well.
- **Hard disk** (type level) – includes all internal hard drives with any connection interface (IDE, SATA, SCSI, etc). DeviceLock treats all external USB, FireWire and PCMCIA hard drives as the **Removable** type. Also, DeviceLock treats as **Removable** some internal hard drives (usually SATA and SCSI) if they support the hot plug feature and Windows is not installed and running on them.

  Note: Even if you deny access to the Hard disk type, users with local administrative privileges (the SYSTEM user and members of the local Administrators group) still can access the partition where Windows is installed and running.

- **Infrared port** (interface level) – includes all devices that can be connected to the computer via the infrared (IrDA) port.
- **iPhone** (type level) – includes all iPhone, iPod Touch, and iPad devices. DeviceLock controls iPhone, iPod Touch, and iPad devices that are working with a PC through the iTunes application or its API.
- **MTP** (type level) – includes all devices (such as Android smartphones, etc.) that are working with a PC through the Media Transfer Protocol.
- **Optical Drive** (type level) – includes all internal and external CD/DVD/BD devices (readers and writers) with any connection interface (IDE, SATA, USB, FireWire, PCMCIA, etc).
- **Palm** (type level) – includes all Palm OS devices with any type of connection interface (USB, COM, IrDA, Bluetooth, WiFi) to the computer. DeviceLock controls Palm OS devices that are working with a PC through the HotSync application.
- **Parallel port** (interface level) – includes all devices that can be connected to the computer via the parallel (LPT) ports.
- **Printer** – (type level) – includes all local and network printers with any type of connection interface (USB, LPT, Bluetooth, etc) to the computer. DeviceLock can

even optionally control virtual printers which do not send documents to real devices, but instead print to files (for example, PDF converters).

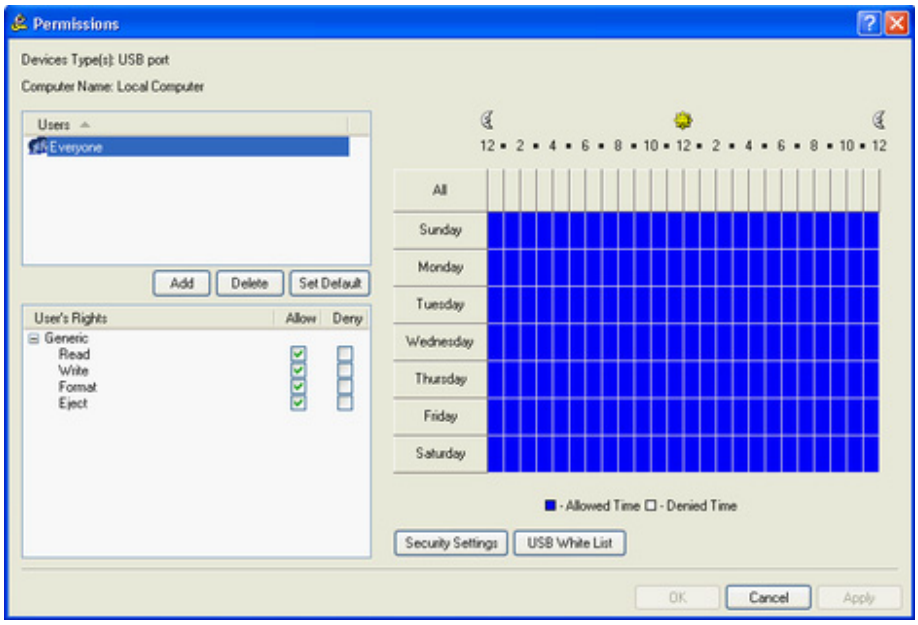
- **Removable** (type level) – includes all internal and external devices with any connection interface (USB, FireWire, PCMCIA, IDE, SATA, SCSI, etc) that are recognized by Windows as removable devices (for example, USB flash drives, ZIP drives, card readers, magneto-optical drives, and so on). DeviceLock treats all external USB, FireWire and PCMCIA hard drives as the **Removable** type as well. Also, DeviceLock treats as **Removable** some internal hard drives (usually SATA and SCSI) if they support the hot plug feature and Windows is not installed and running on them.
- **Serial port** (interface level) – includes all devices that can be connected to the computer via the serial (COM) ports, including internal modems.
- **Tape** (type level) – includes all internal and external tape drives with any connection interface (SCSI, USB, IDE, etc).
- **TS Devices** (interface level) – includes mapped drives (all hard, removable and optical drives), serial ports, USB devices and the clipboard redirected from remote terminals to virtual application or desktop sessions, as well as to virtual desktops that run in the server host environment. DeviceLock controls device, port and terminal clipboard redirections via Microsoft RDP, Citrix ICA, VMware PCoIP, HTML5/WebSockets remoting protocols in Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer and VMware View virtualization environments. In addition, for a guest Windows system that runs in VMware Workstation, VMware Player, Oracle VM VirtualBox or Windows Virtual PC virtualization solutions DeviceLock controls data copy operations between its Windows Clipboard and the clipboard of the host operating system.
- **USB port** (interface level) – includes all devices that can be plugged into the USB port, except the hub devices.
- **WiFi** (type level) – includes all internal and external WiFi devices with any type of connection interface (USB, PCMCIA, etc.) to the computer.

  Note: Using the WiFi type you can control user access to the hardware device but not to the network.

- **Windows Mobile** (type level) – includes all Windows Mobile devices with any type of connection interface (USB, COM, IrDA, Bluetooth, WiFi) to the computer. DeviceLock controls Windows Mobile devices that are working with a PC through the Windows Mobile Device Center (WMDC) or Microsoft ActiveSync application or its API.

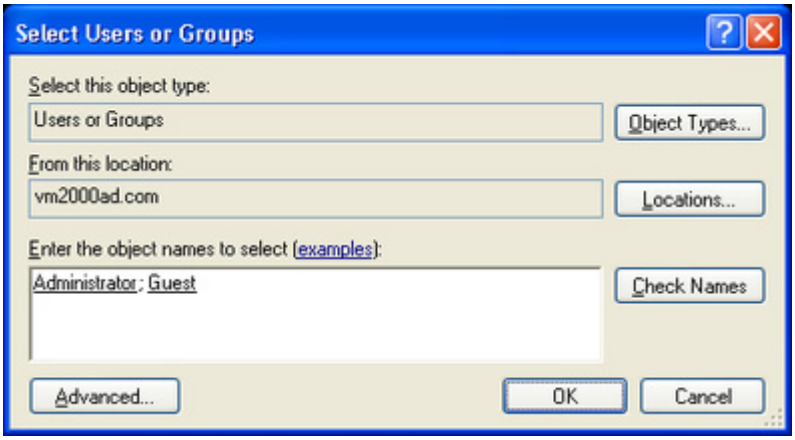
Note: You can define different online vs. offline permissions for the same user or sets of users. Online permissions (Regular Profile) apply to client computers that are working online. Offline permissions (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to set offline permissions, see "Managing Offline Permissions."

To set online (regular) permissions for a device type, highlight it (use Ctrl and/or Shift to select several types simultaneously) and select **Set Permissions** from the context menu available by a right mouse click. Alternatively, you can press the appropriate button on the toolbar.



The names of the users and user groups assigned to a device type are shown in the list of accounts on the top left-hand side of the **Permissions** dialog box.

To add a new user or user group to the list of accounts, click **Add**. You can add several accounts simultaneously.



To delete a record from the list of accounts, use the **Delete** button. Using CTRL and/or SHIFT you can select and remove several records simultaneously.

Use the **Set Default** button to set default permissions for devices. Default permissions are enabled by using the following access selections:

ACCOUNT/ DEVICE TYPE	EVERYONE	ADMINISTRATORS	SYSTEM
BlackBerry	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Bluetooth	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Clipboard	Generic: Copy to clipboard Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content	Generic: Copy to clipboard Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content	Generic: Copy to clipboard Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content
FireWire port	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
Floppy	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
Hard disk	Generic: Read, Write	Generic: Read, Write, Format	Generic: Read, Write, Format
Infrared port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
iPhone	Generic: Read, Write, Modem	Generic: Read, Write, Modem	Generic: Read, Write, Modem
MTP	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Optical Drive	Generic: Read, Write, Eject	Generic: Read, Write, Eject	Generic: Read, Write, Eject
Palm	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Parallel port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Printer	Generic: Print	Generic: Print	Generic: Print
Removable	Generic: Read, Write, Eject Encrypted: Read, Write, Format	Generic: Read, Write, Format, Eject Encrypted: Read, Write, Format	Generic: Read, Write, Format, Eject Encrypted: Read, Write, Format
Serial port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Tape	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
TS Devices	Generic: Mapped Drives Read, Serial Port Access, USB	Generic: Mapped Drives Read, Mapped Drives Write, Serial	Generic: Mapped Drives Read, Mapped Drives

ACCOUNT/ DEVICE TYPE	EVERYONE	ADMINISTRATORS	SYSTEM
	Devices Access, Clipboard Incoming Text, Clipboard Incoming Image, Clipboard Incoming Audio, Clipboard Incoming File, Clipboard Incoming Unidentified Content	Port Access, USB Devices Access, Clipboard Incoming Text, Clipboard Outgoing Text, Clipboard Incoming Image, Clipboard Outgoing Image, Clipboard Incoming Audio, Clipboard Outgoing Audio, Clipboard Incoming File, Clipboard Outgoing File, Clipboard Incoming Unidentified Content, Clipboard Outgoing Unidentified Content	Write, Serial Port Access, USB Devices Access, Clipboard Incoming Text, Clipboard Outgoing Text, Clipboard Incoming Image, Clipboard Outgoing Image, Clipboard Incoming Audio, Clipboard Outgoing Audio, Clipboard Incoming File, Clipboard Outgoing File, Clipboard Incoming Unidentified Content, Clipboard Outgoing Unidentified Content
USB port	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
WiFi	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Windows Mobile	Generic: Read, Write, Execute	Generic: Read, Write, Execute	Generic: Read, Write, Execute

Using special time control, you can define a time when the selected user or user group will or will not have access to devices. Time control appears at the top-right side of the **Permissions** dialog box. Use the left mouse button and select the allowed time. To select a denied time use the right mouse button. Also, you can use the keyboard to set times – arrow keys for navigation and the spacebar to toggle allowed/denied time.

To define which actions on devices are to be allowed or denied for a user or user group, set the appropriate rights. All rights are divided into three groups: **Generic**, **Encrypted**, and **Special Permissions**. Each group has its own set of rights:

- **Generic** – Generic rights do not apply to devices that are recognized by DeviceLock Service as encrypted devices. For more information on encryption integration, please read the Encryption section of this manual.
    - **Read** – to enable data reading from the device. Applies to all device types except Clipboard and Printer.
    - **Write** – to enable data writing to the device. With the exception of Windows Mobile, this right can be enabled for all devices only if **Read** is selected in the **Generic** group. It cannot be disabled for BlackBerry, Bluetooth, Infrared port, Parallel port, Serial port and WiFi device types. When **Write** is disabled for USB and FireWire ports it has the following effects: storage devices such as flash drives, floppies, hard disks, optical drives, etc. can be read, but not

written to; non-storage devices such as printers, scanners, etc. cannot be accessed.

- **Format** – to enable the formatting, checking, and any other direct access of drives. You can enable this right only if **Read** is selected in the **Generic** group. Applies only to FireWire port, Floppy, Hard disk, Removable and USB port device types. When this right is enabled for USB and FireWire ports it affects only storage devices plugged into these ports.
- **Eject** – to enable ejection of the media. You can enable this right only if **Read** is selected in the **Generic** group. This right controls only ejection via software. Hardware ejection using the eject button on a device's front panel cannot be prevented. Applies only to FireWire port, Floppy, Optical Drive, Removable and USB port device types. When this right is enabled for USB and FireWire ports it affects only storage devices plugged into these ports.
- **Execute** – to enable the remote code execution on the device's side. Applies only to the Windows Mobile device type.
- **Modem** – to enable use the Internet Tethering feature. Applies only to the iPhone device type.
- **Print** – to enable document printing. Applies only to the Printer device type.
- **Copy to clipboard** – to enable data pasting from the clipboard. Applies only to the Clipboard device type. This right automatically grants full access to the clipboard.
- **Mapped Drives Read** – to enable data reading from mapped drives during a terminal session. Applies only to TS Devices.
- **Mapped Drives Write** – to enable data writing to mapped drives during a terminal session. Applies only to TS Devices.
- **Serial Port Access** – to enable access to serial ports during a terminal session. Applies only to TS Devices.
- **USB Devices Access** – to enable access to USB devices during a terminal session. Applies only to TS Devices.
- **Clipboard Incoming Text** – to enable pasting text data from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing Text** – to enable pasting text data from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Incoming Image** – to enable pasting graphical data from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing Image** – to enable pasting graphical data from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Incoming Audio** – to enable pasting audio data from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing Audio** – to enable pasting audio data from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Incoming File** – to enable pasting files from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing File** – to enable pasting files from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Incoming Unidentified Content** – to enable pasting any other uncategorized content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.

    - **Clipboard Outgoing Unidentified Content** – to enable pasting any other uncategorized content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
- **Encrypted** – encrypted rights only apply to devices that are recognized by DeviceLock Service as encrypted devices. For more information on encryption integration, please read the Encryption section of this manual.
    - **Read** – to enable data reading from an encrypted device. Applies only to the Removable device type.
    - **Write** – to enable data writing to an encrypted device. You can enable this right only if **Read** is selected in the **Encrypted** group. Applies only to the Removable device type.
    - **Format** – to enable the formatting, checking, and any other direct access of encrypted drives. You can enable this right only if **Read** is selected in the **Encrypted** group. Applies only to the Removable device type.
- **Special Permissions** – these rights only apply to iPhone, Windows Mobile, Palm and Clipboard device types. The content types (*Calendar*, *Contacts*, *Tasks*, etc.) that are controlled by these rights for iPhone, Windows Mobile, and Palm devices represent the same content types that exist in iTunes, HotSync, Microsoft ActiveSync and WMDC applications. For Palm devices, you can enable any **Write** right only if the corresponding **Read** right is also enabled.
    - **Read Calendar** – to enable reading the calendar on a mobile device from a PC.
    - **Write Calendar** – to enable writing to a calendar on a mobile device from a PC.
    - **Read Contact** – to enable reading contacts on a mobile device from a PC.
    - **Write Contact** – to enable writing contacts from a PC to a mobile device.
    - **Read E-mail** – to enable reading e-mails on a mobile device from a PC. For iPhone, this content type represents e-mail account settings but not messages because iTunes does not support sync of messages.
    - **Write E-mail** – to enable writing e-mails from a PC to a mobile device. For iPhone, this content type represents e-mail account settings but not messages because iTunes does not support sync of messages.
    - **Read Attachment** – to enable reading e-mail attachments on a Windows Mobile device from a PC. You can enable this right only if **Read E-mail** is selected in the **Special Permissions** group.
    - **Write Attachment** – to enable writing e-mail attachments from a PC to a Windows Mobile device. You can enable this right only if **Write Email** is selected in the **Special Permissions** group.
    - **Read Favorite** – to enable reading favorites on a Windows Mobile device and iPhone from a PC.
    - **Write Favorite** – to enable writing favorites from a PC to a Windows Mobile device and iPhone.
    - **Read File** – to enable reading files on a mobile device from a PC. For iPhone, data flows of the *Applications* iTune's type are treated as files.
    - **Write File** – to enable writing files from a PC to a mobile device. For a Palm device this right also enables **Write Document** in the **Special Permissions** group. For iPhone, data flows of the *Applications* iTune's type are treated as files.

- **Read Media** – to enable reading media content using Windows Media Player on a Windows Mobile device and reading media files on a Palm device and iPhone from a PC. You can enable this right only if **Read Files** is selected in the **Special Permissions** group. For a Windows Mobile device, this option also requires selecting **Execute** from the **Generic** group. For iPhone, the media content type consists of the following iTunes types: *Ringtones*, *Music*, *Audiobooks*, *Photos*, *Podcasts* (Audio & Video), *Movies*, *TV shows*, *Rented Movies*.
- **Write Media** – to enable writing media content using Windows Media Player to a Windows Mobile device and writing media files to a Palm device and iPhone from a PC. You can enable this right only if **Write Files** is selected in the **Special Permissions** group and, for a Windows Mobile device, if **Execute** is selected from the **Generic** group. For iPhone, the media content type consists of the following iTunes types: *Ringtones*, *Music*, *Audiobooks*, *Photos*, *Podcasts* (Audio & Video), *Movies*, *TV shows*, *Rented Movies*.
- **Read Backup** – to enable creating the iPhone backup by reading the device data from a PC.

Note: An iPhone device is backed up by iTunes each time users sync with iTunes (automatically on the first sync, every time they connect it to the computer). To allow synchronization to complete successfully, grant the **Read Backup** permission to users for the **iPhone** device type. Otherwise, if iTunes automatically creates an iPhone backup, the synchronization session will be interrupted.

To avoid interrupting the synchronization process, users should set iTunes to sync only the content to which they are allowed access.

- **Write Backup** – to enable restoring iPhone by writing the device backup data from a PC.
- **Read Note** – to enable reading notes on a mobile device from a PC. For a Palm device this right controls *Memos* and *Note Pad* content types.
- **Write Note** – to enable writing notes from a PC to a mobile device. For a Palm device this right controls *Memos* and *Note Pad* content types.
- **Read Pocket Access** – to enable reading Pocket Access databases on a Windows Mobile device from a PC.
- **Write Pocket Access** – to enable writing Pocket Access databases from a PC to a Windows Mobile device.
- **Read Task** – to enable reading tasks on a mobile device from a PC.
- **Write Task** – to enable writing tasks from a PC to a mobile device.
- **Read Expense** – to enable reading Palm Expense application data on a Palm device from a PC.
- **Write Expense** – to enable writing Palm Expense application data from a PC to a Palm device.
- **Read Document** – to enable reading Palm documents on a Palm device from a PC. You can enable this right only if **Read Files** is selected in the **Special Permissions** group.
- **Write Document** – to enable writing Palm documents from a PC to a Palm device. You can enable this right only if **Write Files** is selected in the **Special Permissions** group.
- **Read Unidentified Content** – to enable reading any other uncategorized content type on a Windows Mobile device from a PC.
- **Write Unidentified Content** – to enable writing any other uncategorized content type from a PC to a Windows Mobile device.

- **Copy Text** – to enable pasting text data from the clipboard.
- **Copy Image** – to enable pasting graphical data from the clipboard.
- **Copy Audio** – to enable pasting audio data from the clipboard.
- **Copy File** – to enable pasting files from the clipboard.
- **Screenshot** – to enable capturing screen shots of the entire screen, the active window or any segment of the screen to the clipboard.

Note: Because screen shots captured using screen capture tools and utilities are saved directly to files while screen shots captured by pressing the PRINT SCREEN key are first copied to the clipboard and then must be pasted into a separate program (for example, Microsoft Word or Paint), different access rights are required to control access to screen shots. To allow users to capture screen shots using screen capture tools and utilities, you must grant them only the Screenshot right. To allow users to capture screen shots by pressing the PRINT SCREEN key, you must grant them the Screenshot and Copy Image rights.

If users do not have the Screenshot right, they cannot capture screen shots using the PRINT SCREEN key or screen capture tools and utilities.

- **Copy Unidentified Content** - to enable pasting any other uncategorized content type from the clipboard.

Note: The Copy Text, Copy Image, Copy Audio, Copy File, and Copy Unidentified Content rights do not control data copying to the clipboard. Users can always copy data to the clipboard regardless of the rights they have.

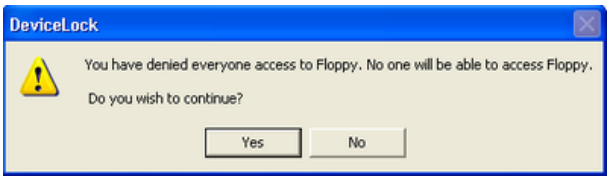
Note: If the access (read and/or write) to some content type is denied during the iPhone or Windows Mobile synchronization process, you have to replug the device in order to continue using the iPhone or Windows Mobile device.

When users attempt to synchronize a Palm handheld device over a network and DeviceLock denies access to some content type, the synchronization session is interrupted. To avoid this situation, users should set the HotSync application to sync only the content to which they are allowed access before attempting synchronization.

If all **Allow** rights are enabled for the user account it means that this account has "full access" rights. If all **Deny** rights are enabled for the user account it means that this account has "no access" rights. If neither **Allow** nor **Deny** rights are enabled for the user account it means that this account inherits access rights from its user group (if there is no group to inherit rights from then this account has "no access" rights).

Note: The "no access" right has a priority over all other rights. It means that if the group to which some user belongs has the "no access" right but this user has "full access", the user still cannot access a device. If you want to deny access for some user or group, you can just remove it from the account's list, it is not necessary to add it with "no access".

Also, the Everyone user has a priority over all other accounts. It means that if Everyone has the "no access" right, no one can access a device.

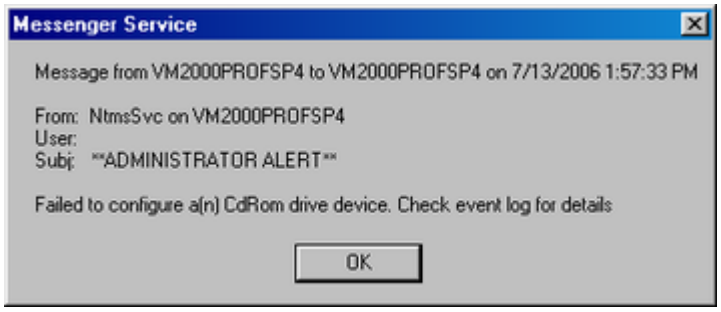


Even if you deny access to hard disks, users with local administrative privileges (the SYSTEM user and members of the local Administrators group) still can access the partition where Windows is installed and running.

We recommend that you add only those accounts (users and/or groups) to the list which should be able to access a device. If the account's list is empty (contains no records at all) then no one can access a device.

Also, it is recommended to add the SYSTEM user with "full access" to hard disks and optical drives.

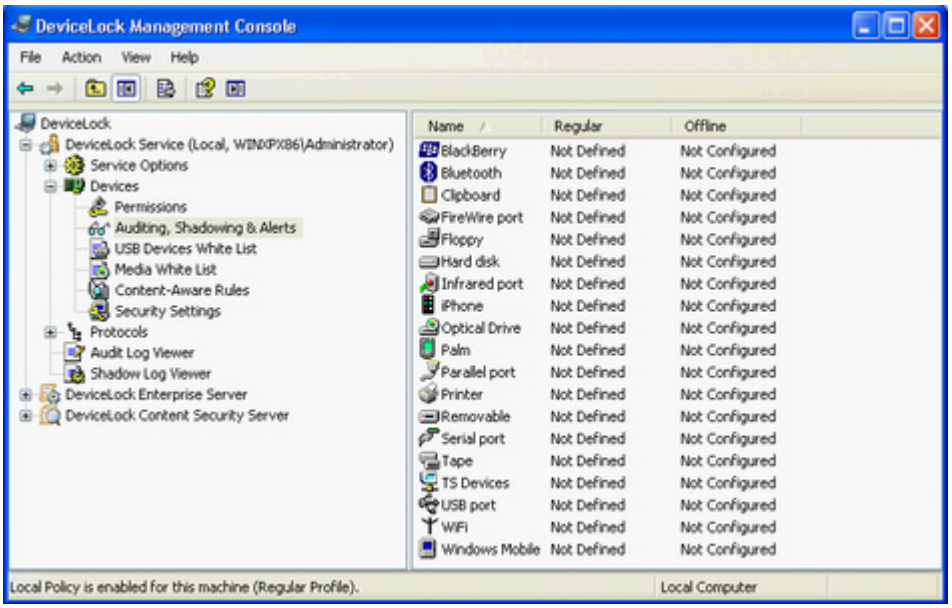
On some systems, users may receive the following message when they log in.


Messenger Service
Message from VM2000PROFSP4 to VM2000PROFSP4 on 7/13/2006 1:57:33 PM
From: NtmsSvc on VM2000PROFSP4
User:
Subj: **ADMINISTRATOR ALERT**
Failed to configure a(n) CdRom drive device. Check event log for details
OK

It means that the SYSTEM user cannot access DVD/CD/BD-ROM. To avoid this message, set the "full access" right for SYSTEM on Optical Drive.

Auditing, Shadowing & Alerts (Regular Profile)

There is a list of device types for which you can define user-level audit, shadowing rules and alerts.


DeviceLock Management Console
File Action View Help
DeviceLock
DeviceLock Service (Local, WINXPX86\Administrator)
Service Options
Devices
Permissions
Auditing, Shadowing & Alerts
USB Devices White List
Media White List
Content-Aware Rules
Security Settings
Protocols
Audit Log Viewer
Shadow Log Viewer
DeviceLock Enterprise Server
DeviceLock Content Security Server
Name
Regular
Offline
BlackBerry Not Defined Not Configured
Bluetooth Not Defined Not Configured
Clipboard Not Defined Not Configured
FireWire port Not Defined Not Configured
Floppy Not Defined Not Configured
Hard disk Not Defined Not Configured
Infrared port Not Defined Not Configured
iPhone Not Defined Not Configured
Optical Drive Not Defined Not Configured
Palm Not Defined Not Configured
Parallel port Not Defined Not Configured
Printer Not Defined Not Configured
Removable Not Defined Not Configured
Serial port Not Defined Not Configured
Tape Not Defined Not Configured
TS Devices Not Defined Not Configured
USB port Not Defined Not Configured
WiFi Not Defined Not Configured
Windows Mobile Not Defined Not Configured
Local Policy is enabled for this machine (Regular Profile).
Local Computer

There is not much difference between setting up permissions and defining audit, shadowing rules and alerts so at first read the Permissions section of this manual.

DeviceLock Service can use the standard Windows event logging subsystem to log a device's information. It is extremely useful for system administrators because they can use any event log reading software to view the DeviceLock audit log. You can use the standard Event Viewer, for example. Also, DeviceLock Service can use its own protected proprietary log. The data from this log is sent to DeviceLock Enterprise Server and stored centrally in the database. To define what log should be used, set the **Audit log type** parameter in Service Options.

DeviceLock Management Console has its own built-in audit log viewer that represents information from the event log in a more convenient form. For more information, see "Audit Log Viewer (Service)."

To view the audit log stored on DeviceLock Enterprise Server, use the server's audit log viewer.

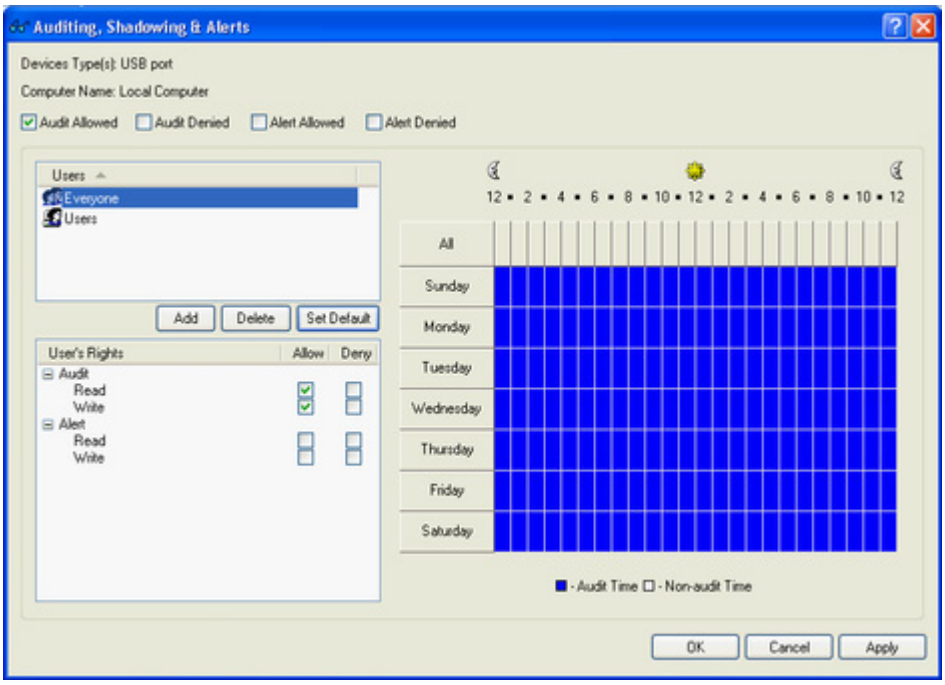
Also there is an extended audit's feature called data shadowing – the ability to mirror all data copied to external storage devices or transferred through serial and parallel ports. A full copy of the data is logged. The shadow log is stored locally in the special directory (see "Service Options") and then can be transferred to the DeviceLock Enterprise Server specified in Service Options to store it in the SQL database.

To view the locally stored shadow log, use DeviceLock Management Console's built-in shadow log viewer. For more information, see "Shadow Log Viewer (Service)."

To view the shadow log stored on DeviceLock Enterprise Server, use the server's shadow log viewer.

Note: You can define different online vs. offline audit and shadowing rules for the same user or sets of users. Online audit and shadowing rules (Regular Profile) apply to client computers that are working online. Offline audit and shadowing rules (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define offline audit and shadowing rules, see "Managing Offline Audit, Shadowing and Alerts."

To define online (regular) audit and shadowing rules for a device type, highlight it (use Ctrl and/or Shift to select several types simultaneously) and select **Set Auditing, Shadowing & Alerts** from the context menu available by the right mouse click. Alternatively, you can press the appropriate button on the toolbar.



There are two types of user access that can be logged to the audit log:

- **Allowed** – all access attempts that were permitted by DeviceLock Service, that is, the user was able to access a device.
- **Denied** – all access attempts that were blocked by DeviceLock Service, that is, the user was not able to access a device.

To enable logging to the audit log for one or both of these access types, check **Audit Allowed** and/or **Audit Denied**. These flags are not linked to users/groups, they are related to a whole device type.

The names of the users and user groups assigned to a device type are shown in the list of accounts on the top left-hand side of the **Auditing, Shadowing & Alerts** dialog box.

To add a new user or user group to the list of accounts, click **Add**. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the **Delete** button. Using CTRL and/or SHIFT you can select and remove several records simultaneously.

Use the **Set Default** button to set default audit and shadowing rules for devices: members of the Users group and the Everyone account have **Read** and **Write** audit rights and shadowing is disabled for them.

Using special time control, you can define a time when the audit rule for the selected user or user group will or will not be active. Time control appears at the top-right side of the **Auditing, Shadowing & Alerts** dialog box. Use the left mouse button and select the time when the rule is active (audit time). To select a time when the rule is not active (non-audit

time), use the right mouse button. Also, you can use the keyboard to set times – arrow keys for navigation and the spacebar to toggle audit/non-audit time.

To define which user's actions on devices are allowed or denied to be logged to either the audit or shadow log, set the appropriate audit rights. All rights are divided into two groups: **Audit** and **Shadowing**. Each group has its own set of rights:

- **Audit** – rights that belong to this group are responsible for actions logged into the audit log.
  - **Read** – to log the read access attempts. For BlackBerry, Bluetooth, FireWire port, Infrared port, Parallel port, Serial port, USB port and WiFi device types, you can enable this right only if **Write** is selected in the **Audit** group.
  - **Write** – to log the write access attempts. For BlackBerry, Bluetooth, FireWire port, Infrared port, Parallel port, Serial port, USB port and WiFi device types, you can enable this right only if **Read** is selected in the **Audit** group.
  - **Format** – to log the direct write access attempts (e.g. formatting). Applies only to Floppy, Hard disk and Removable device types.
  - **Print** – to log all attempts to send documents to printers. Applies only to the Printer device type.
  - **Execute** – to log access attempts to remotely execute a code on the device's side. Applies only to the Windows Mobile device type.
  - **Read Non-files** – to log the read access attempts for non-file objects (*Calendar*, *Contacts*, *Tasks,* etc.). Applies only to iPhone, Windows Mobile and Palm device types.
  - **Write Non-files** – to log the write access attempts for non-file objects (*Calendar*, *Contacts*, *Tasks*, etc.). Applies only to iPhone, Windows Mobile and Palm device types.
  - **Copy** – to log all attempts to paste data from the clipboard and capture screen shots. Applies only to Clipboard.
  - **Mapped Drives Read** – to log all attempts to read data from mapped drives during a terminal session. Applies only to TS Devices.
  - **Mapped Drives Write** – to log all attempts to write data to mapped drives during a terminal session. Applies only to TS Devices.
  - **Serial Port Access** – to log all attempts to access serial ports during a terminal session. Applies only to TS Devices.
  - **USB Devices Access** – to log all attempts to access USB devices during a terminal session. Applies only to TS Devices.
  - **Clipboard Incoming** – to log all attempts to paste clipboard data (text data, graphical data, audio data, files and any other unidentified data) to a terminal session/virtual machine. Applies only to TS Devices.
  - **Clipboard Outgoing** – to log all attempts to paste clipboard data (text data, graphical data, audio data, files and any other unidentified data) from a terminal session/virtual machine. Applies only to TS Devices.
- **Shadowing** – rights that belong to this group are responsible for actions logged into the shadow log.
  - **Read** – to enable shadowing of all data read by the user. Applies only to MTP.
  - **Write** – to enable shadowing of all data written by the user. Applies only to Floppy, iPhone, MTP, Optical Drive, Parallel port, Removable, Serial port, Windows Mobile and Palm device types.

- **Format** – to enable shadowing of raw data written by the user via the direct disk access (e.g. formatting). Applies only to Floppy and Removable device types.
- **Print** – to enable shadowing of all documents sent to printers. Later, these documents can be viewed using any PDF reading software (e.g. Adobe Acrobat Reader) and DeviceLock Printer Viewer. Applies only to the Printer device type.
- **Write Non-files** – to enable shadowing of all non-file objects (Calendar, Contacts, Tasks, etc.) written by the user. Applies only to iPhone, Windows Mobile and Palm device types.
- **Mapped Drives Write** – to enable shadowing of all data written by the user. Applies only to TS Devices.
- **Copy** – to enable shadowing of pasted clipboard data and captured screen shots. Applies only to Clipboard.
- **Clipboard Incoming** – to enable shadowing of clipboard data pasted to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing** – to enable shadowing of clipboard data pasted from a terminal session/virtual machine. Applies only to TS Devices.

Below you can see what audit rights can be assigned to what device types and what is written to the log. For all events DeviceLock Service logs event's type, date and time, device's type, reason (the cause of the event), user name and process information as well as the specific event's information described below:

DEVICE TYPE	RIGHTS
BlackBerry	• Audit: Read **+** *Device Access action is written to the audit log*. • Audit: Write/Print **+** *Device Access action is written to the audit log*.
Bluetooth	• Audit: Read **+** *Device Access action is written to the audit log*. • Audit: Write/Print **+** *Device Access action is written to the audit log*.
Clipboard	• Audit: Copy **+** *Copy Text, Copy File, Copy Image, Copy Audio, Copy Unidentified, Screenshot actions, file names and flags (process name and PID) are written to the audit log*. • Shadowing: Copy **+** *All data placed on the clipboard are written to the shadow log.*
FireWire port	• Audit: Read **+** *Insert, Remove and Device Access actions, device names and flags (Device ID, Read Write) write to the audit log*. • Audit: Write/Print **+** *Insert, Remove and Device Access actions, device names and flags (Device ID, Read Write) write to the audit log*.
Floppy	• Audit: Read **+** *Mount, Unmount and Read actions and file names write to the*

DEVICE TYPE	RIGHTS
	audit log. • Audit: Write/Print **+** *Delete, Write, Restore and Rename actions and file names write to the audit log*. • Audit: Format **+** *Format action and disk name write to the audit log*. • Shadowing: Write/Print **+** *Files are written to the shadow log*. • Shadowing: Format **+** *Raw data is written to the shadow log.*
Hard disk	• Audit: Read **+** *Read action and file names write to the audit log*. • Audit: Write/Print **+** *Write, Rename and Delete actions and file names write to the audit log*. • Audit: Format **+** *Format action and disk name write to the audit log*.
Infrared port	• Audit: Read **+** *Device Access action writes to the audit log*. • Audit: Write/Print **+** *Device Access action writes to the audit log*.
iPhone	• Audit: Read **+** *Read File action and file names write to the audit log*. • Audit: Write/Print **+** *Write File, Rename File and Delete File actions and file names write to the audit log*. • Audit: Read Non-files **+** *Read Calendar, Read Contact, Read Favorite, Read E-mail, Read Backup, Read Note and Read Media actions and object names write to the audit log*. • Audit: Write Non-files **+** *Write Calendar, Delete Calendar, Write Contact, Delete Contact, Write Favorite, Delete Favorite, Write E-mail, Delete E-mail, Write Backup, Write Note, Delete Note, Write Media, Rename Media and Delete Media actions and object names write to the audit log*. • Shadowing: Write/Print **+** *Files are written to the shadow log*. • Shadowing: Write Non-files **+** *All data that contains non-file objects (Calendar, Contacts, etc.) is written to the shadow log*.

DEVICE TYPE	RIGHTS
MTP	• Audit: Read + *Read action and file names write to the audit log*. • Audit: Write/Print + *Delete, Rename and Write actions and file names write to the audit log*. • Shadowing: Read + *Files are written to the shadow log*. • Shadowing: Write/Print + *Files are written to the shadow log*.
Optical Drive	• Audit: Read **+** *Read, Mount, Unmount and Eject actions and file names write to the audit log*. • Audit: Write/Print **+** *Write and Format actions and file names write to the audit log*. • Shadowing: Write/Print **+** *CD/DVD/BD images in the CUE format and/or files write to the shadow log*.
Palm	• Audit: Read **+** *Read File action, file names and the Sync flag write to the audit log*. • Audit: Write/Print **+** *Write File action, file names and the Sync flag write to the audit log*. • Audit: Read Non-files **+** *Read Calendar, Read Contact, Read Expense, Read E-mail, Read Document, Read Memo, Read Notepad, Read Task and Read Media actions and object names write to the audit log*. • Audit: Write Non-files **+** *Write Calendar, Write Contact, Write Expense, Write E-mail, Write Document, Write Memo, Write Notepad, Write Task, Write Media and Install actions and object names write to the audit log*. • Shadowing: Write/Print **+** *Files are written to the shadow log*. • Shadowing: Write Non-files **+** *All data that contains non-file objects (Calendar, Contacts, Tasks, etc.) is written to the shadow log*.
Parallel port	• Audit: Read **+** *Device Access action writes to the audit log*. • Audit: Write/Print **+** *Device Access action writes to the audit log*. • Shadowing: Write/Print **+**

DEVICE TYPE	RIGHTS
	All data sent to the port is written to the shadow log.
Printer	• Audit: Write/Print **+** *Print action, documents and printer names write to the audit log*. • Shadowing: Write/Print **+** *All data sent to the printer is written to the shadow log in the PDF format*.
Removable	• Audit: Read **+** *Read, Read Encrypted, Eject, Mount and Unmount actions and file names write to the audit log*. • Audit: Write/Print **+** *Delete, Delete Encrypted, Rename, Rename Encrypted, Write, Write Encrypted, Restore and Restore Encrypted actions and file names write to the audit log*. • Audit: Format **+** *Format, Format Encrypted actions and disk name write to the audit log*. • Shadowing: Write/Print **+** *Files are written to the shadow log*. • Shadowing: Format **+** *Raw data is written to the shadow log.*
Serial port	• Audit: Read **+** *Device Access action writes to the audit log*. • Audit: Write/Print **+** *Device Access action writes to the audit log*. • Shadowing: Write/Print **+** *All data sent to the port is written to the shadow log*.
Tape	• Audit: Read **+** *Read, Eject actions and device names write to the audit log*. • Audit: Write/Print **+** *Write action and device names write to the audit log*.
TS Devices	• Audit: Mapped Drives Read **+** *Read action, drive name and path to the file are written to the audit log*. • Audit: Mapped Drives Write **+** *Write action, drive name and path to the file are written to the audit log*. • Audit: Serial Port Access **+** *Device Access action and name of the serial port are written to the audit log*. • Audit: USB Devices Access **+** *Device Access action and device name are written to the audit log*. • Audit: Clipboard Incoming **+**

DEVICE TYPE	RIGHTS
	Incoming Text, Incoming Image, Incoming Audio, Incoming File, Incoming Unidentified actions, the file name or data object name and flags (process name and PID) are written to the audit log. • Audit: Clipboard Outgoing **+** *Outgoing Text, Outgoing Image, Outgoing Audio, Outgoing File, Outgoing Unidentified actions, the file name or data object name and flags (process name and PID) are written to the audit log*. • Shadowing: Clipboard Incoming **+** *All data pasted from the clipboard are written to the shadow log*. • Shadowing: Clipboard Outgoing **+** *All data placed on the clipboard are written to the shadow log*.
USB port	• Audit: Read **+** *Insert, Remove and Device Access actions, device names and flags (Device ID, Read Write) write to the audit log*. • Audit: Write/Print **+** *Insert, Remove and Device Access actions, device names and flags (Device ID, Read Write) write to the audit log*.
WiFi	• Audit: Read **+** *Device Access action writes to the audit log*. • Audit: Write/Print **+** *Device Access action writes to the audit log*.
Windows Mobile	• Audit: Read **+** *Read File action, file names and flag (Sync) write to the audit log*. • Audit: Write/Print **+** *Write File, Delete File, Rename, Overwrite and Create Shortcut actions, file names and flags write to the audit log*. • Audit: Execute **+** *Invoke and Execute actions, file names and function (procedure) names write to the audit log*. • Audit: Read Non-files **+** *Read Calendar, Read Contact, Read Favorite, Read E-mail, Read Attachment, Read Note, Read Task, Read Media, Read Pocket Access and Read Unidentified actions and object names write to the audit log*. • Audit: Write Non-files **+** *Write Calendar, Delete Calendar, Write Contact, Delete Contact, Write Favorite, Delete Favorite, Write E-mail, Delete E-Mail, Write Attachment, Delete Attachment, Write Note, Delete Note, Write Task, Delete Task, Write Media, Delete Media, Write Pocket Access, Delete Pocket Access, Write Unidentified and Delete Unidentified actions and object names write to the audit log*. • Shadowing: Write/Print **+** *Files are written to the shadow log*. • Shadowing: Write Non-files **+**

DEVICE TYPE	RIGHTS
	All data that contains non-file objects (Calendar, Contacts, Tasks, etc.) is written to the shadow log.

Note: Until either **Audit Allowed** or **Audit Denied** is selected for the device type, logging to the audit log is disabled for that device in spite of defined audit rules.

Also logging is disabled for a whole class of devices if the access control for that class is turned off in **Security Settings**.

You can enable alerts that are sent when a specific user attempts to access a specific device type.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for specific events, you must configure alert settings in **Service Options**.

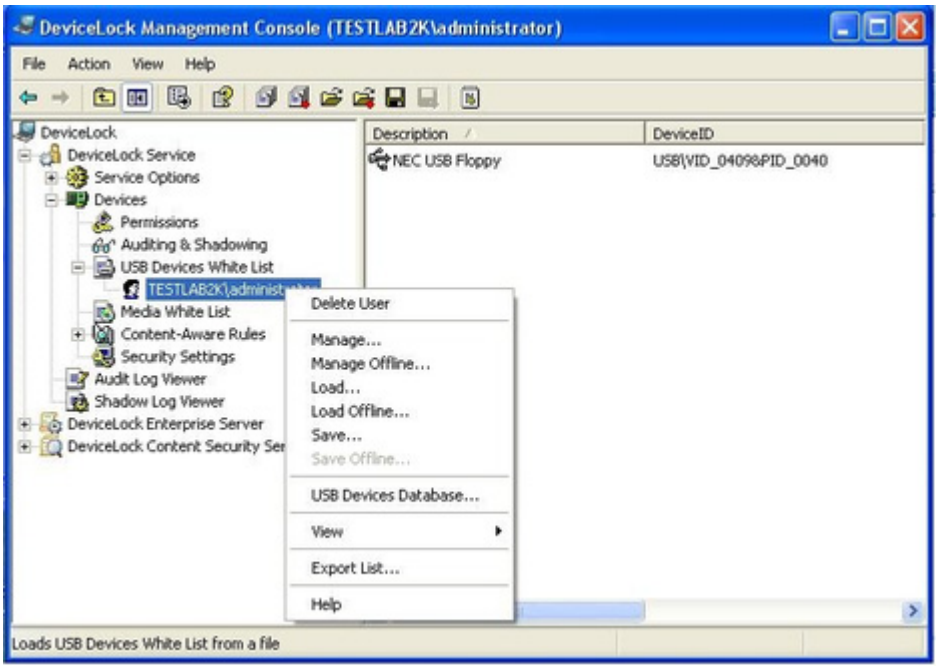
Alerts for specific access-related events are enabled in the **Auditing, Shadowing & Alerts** dialog box. Enabling alerts is similar to defining audit rules and includes the following basic steps:

- Specify which events will trigger alert notifications. You can enable notification of successful and/or failed attempts to access a device. Select the **Alert Allowed** check box to enable notification of successful attempts to access a device. Select the **Alert Denied** check box to enable notification of failed attempts to access a device.
- Specify users and/or groups whose actions will trigger alert notifications. To do so, in the upper-left pane of the dialog box, under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.
- Specify which user's actions on devices either will or will not trigger alert notifications. In the upper-left pane of the dialog box, under **Users**, select the user or group that you added. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny an alert right. Alert rights determine which user actions on devices trigger alert notifications. Alert rights are identical to audit rights. The only difference is that when events matching specific criteria occur DeviceLock triggers alerts instead of logging these events in the Audit Log. For detailed information on Audit rights for devices, see the description of rights earlier in this section.
- Specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on devices either will or will not trigger alert notifications. To do so, in the right pane of the dialog box, use the left mouse button to select days and hours when the selected user's actions on devices will trigger alert notifications. Use the right mouse button to mark days and hours when the selected user's actions on devices will not trigger alert notifications.

Note: You can enable different online vs. offline device type-specific alerts. Online alerts (Regular Profile) are generated when client computers are working online. Offline alerts (Offline Profile) are generated when client computers are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to enable offline alerts, see "Managing Offline Audit, Shadowing and Alerts."

USB Devices White List (Regular Profile)

The devices white list allows you to authorize only specific devices that will not be locked regardless of any other settings. The intention is to allow special devices but lock all other devices.



Devices in the white list can be defined individually for every user and group. For more information on how the devices white list works, please read the Managed Access Control section of this manual.

Note: Audit is not performed for users' attempts to access a whitelisted device while users' attempts to insert or remove a whitelisted device are audited.

There are two ways to identify devices in the white list:

- **Device Model** – represents all devices of the same model. Each device is identified by a combination of Vendor Id (VID) and Product Id (PID).

  This combination of VID and PID describes a unique device model but not a unique device unit. It means that all devices belonging to the certain model of the certain vendor will be recognized as the one authorized device.

- **Unique Device** – represents a unique device unit. Each device is identified by a combination of Vendor Id (VID), Product Id (PID) and Serial Number (SN).

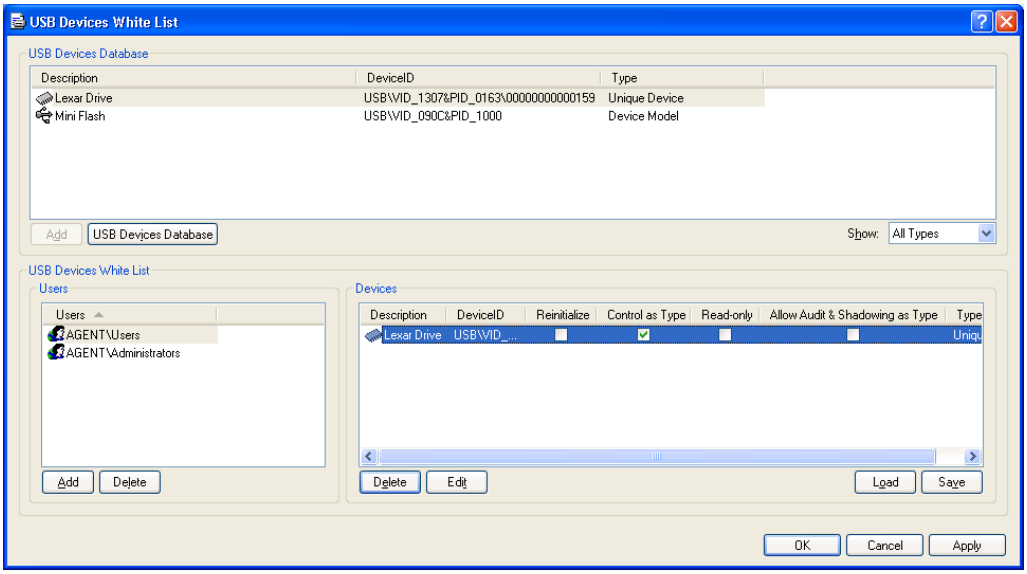
  Not all devices have serial numbers assigned. A device can be added to the white list as a **Unique Device** only if its manufacturer has assigned a serial number to it at the production stage.

Two steps are required to authorize a device:

1. Add the device to the devices database, making it available for adding to the white list.
2. Add the device to the white list for the specified user/group. In effect, this designates the device as authorized and allows it for this user/group at the interface (USB) level.

Note: You can define different online vs. offline USB Devices White Lists for the same user or sets of users. The online USB Devices White List (Regular Profile) applies to client computers that are working online. The offline USB Devices White List (Offline Profile) applies to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define the offline USB Devices White List, see "Managing Offline USB Devices White List."

To define the online (regular) white list, select **Manage** from the context menu available with a right mouse click. Alternatively, you can press the appropriate button on the toolbar.



In the **USB Devices Database** list at the top of the dialog box, you can see devices that were added to the database.

Once devices are added from the database to the white list of a certain user, they become authorized devices for which access control is disabled when this user is logged in.

You can add a device to the USB Devices White List in two steps:

1. Select a user or user group for which this device should be allowed. Click **Add** under the **Users** list to add the user/group. To delete the record from the **Users** list, click **Delete**.
2. Select the appropriate device record in the **USB Devices Database** list and click **Add**.

   If the device has an assigned serial number, it can be added to the white list two times: as Device Type and as Unique Device. In this case Device Type has a priority over Unique Device.

When the **Control as Type** check box is selected, access control for white listed devices is disabled only on the interface (USB) level. If the white listed device (for example, USB Flash Drive) belongs to both levels: interface (USB) and type (Removable), the permissions as well as auditing, shadowing and alerts settings (if any) for the type level will be applied anyway.

Otherwise, if the **Control as Type** check box is not selected, access control on the type level is also disabled. For example, by clearing the **Control as Type** check box for the USB Flash Drive, you can bypass security checking on the Removable level.

Note: When you add a USB composite device (a device that is represented in the system by a parent composite device and one or more child interface devices) to the USB Devices White List, consider the following:

If you add any device of a USB composite device to the white list, access control is disabled for all devices of the composite device at the interface (USB port) level. If the white-listed device belongs to both levels: interface (USB) and type (for example, Removable) and the **Control as Type** check box is selected, the permissions (if any) for the type level will be applied anyway.

When the **Read-only** check box is selected, only read access is granted to the white listed storage device. If this device doesn't support read-only access then access to this device is blocked.

To enable auditing, shadowing and alerting for the white listed device at the type level according to settings defined in Auditing, Shadowing & Alerts (for all device types to which this device belongs to), select the **Allow Audit & Shadowing as Type** check box.

If it is necessary to force the white listed device to reinitialize (replug) when the new user is logged in, select the **Reinitialize** check box.

Some USB devices (like the mouse) will not work without being reinitialized, so it is recommended to keep this check box selected for non-storage devices.

It is recommended to keep the **Reinitialize** check box unselected for storage devices (such as flash drives, optical drives, external hard drives and so on).

Some USB devices cannot be reinitialized from DeviceLock Service. It means that their drivers do not support the software replug. If such a device was white listed but does not work, the user should remove it from the port and then insert it again manually to restart the device's driver.

To edit a device's description, select the appropriate record in **USB Devices White List** and click **Edit**.

Click **Delete** to delete a selected device's record (use CTRL and/or SHIFT to select several records simultaneously).

To save the white list to an external file, click **Save**, and then select the name of the file. To load a previously saved white list, click **Load** and select a file that contains the list of devices.

If you need to manage the devices database, you can click **USB Devices Database** and open the appropriate dialog box.

Note: If you add an iPhone device to the USB Devices White List, access control is disabled for both the iPhone and its camera at the interface (USB port) level. Thus, you cannot allow access to iPhone and deny access to its camera at the interface (USP port) level. In the USB devices database, an iPhone device is identified as the "Apple Mobile Device USB Driver."

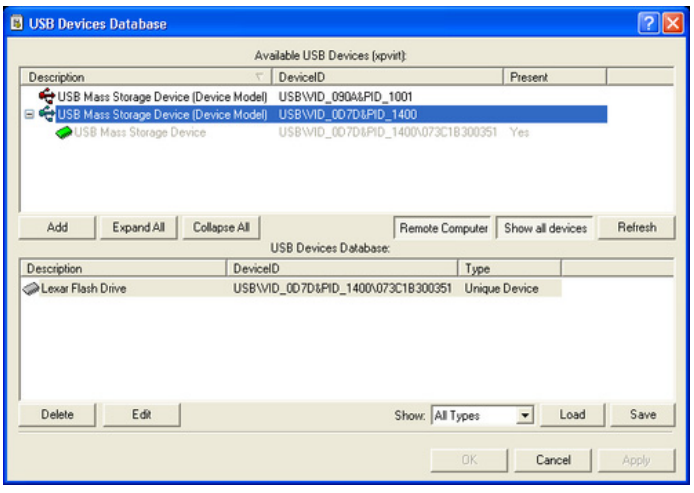
However, it is possible to allow access to iPhone's camera and deny access to iPhone. To do this, you can use any of the following methods:

Method 1. To allow access to iPhone's camera, add the iPhone to the USB Devices White List and select the **Control as Type** check box. To deny access to iPhone, set the No Access permission for the **iPhone** device type.

Method 2. To allow access to iPhone's camera, clear the **Access control for USB scanners and still image devices** check box in **Security Settings**. To deny access to iPhone, set the No Access permission for the **USB port** device type.

USB Devices Database

In the **USB Devices Database** dialog box you can add new devices to the database and edit existing records.



Before the device can be authorized in the white list, it must be added to the database.

In the **Available USB Devices** list at the top of the dialog box, you can see all devices available on the computer.

Devices are displayed in the form of a simple tree, where the parent item represents ***Device Model*** and the child item represents ***Unique Device***. If there is no Unique Device item, then this device does not have an assigned serial number.

This list displays either all currently plugged-in devices (if the **Show all devices** button is not clicked) or all the devices ever plugged into the port on this computer (if the **Show all devices** button is clicked).

The list of available devices is automatically refreshed and displays new devices as soon as they arrive. To manually refresh this list, click **Refresh**.

To retrieve devices from the remote computer, click **Remote Computer**. This button is unavailable when you are connected to the local computer.

In the **USB Devices Database** list at the bottom of the dialog box, you can see devices that are already in the database.

You can add devices to this list by selecting the desired device's record in the **Available USB Devices** list and clicking **Add**. If the device is already in the database, it cannot be added there a second time.

To edit a device description, select the appropriate record in the **USB Devices Database** list and click **Edit**.

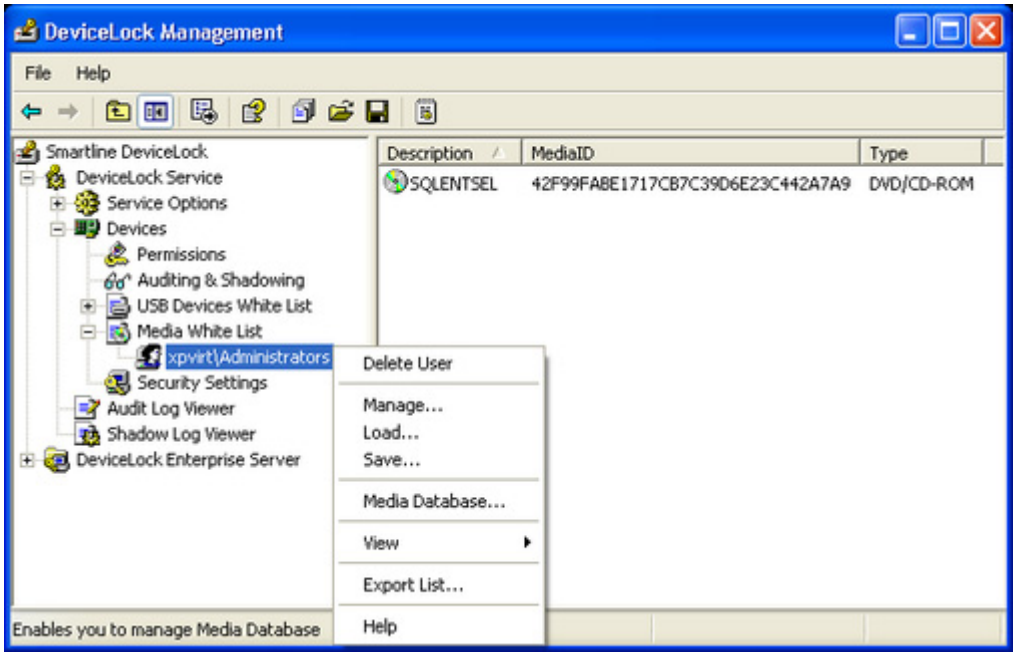
Click **Delete** to delete a selected device's record (press CTRL and/or SHIFT to select several records simultaneously).

You can also save a current database to an external file. To save the database to an external file, click **Save**, then select the type of the file — .txt or .csv.

To load a previously saved database, click **Load** and select a file that contains the list of devices.

Media White List (Regular Profile)

The media white list allows you to uniquely identify a specific CD/DVD/BD-ROM disk by the data signature and authorize read access to it, even when DeviceLock Service has otherwise blocked optical drives.



The media white list can be configured to grant access to a collection of approved CD/DVD/BD-ROM disks by certain users and groups, so that only authorized users are able to use the approved information.

Any change to the content of the media will change the data signature, thus invalidating authorization. If the user copies the authorized media without any changes in the original content (byte-to-byte copy) then such a copy is accepted as the authorized media.

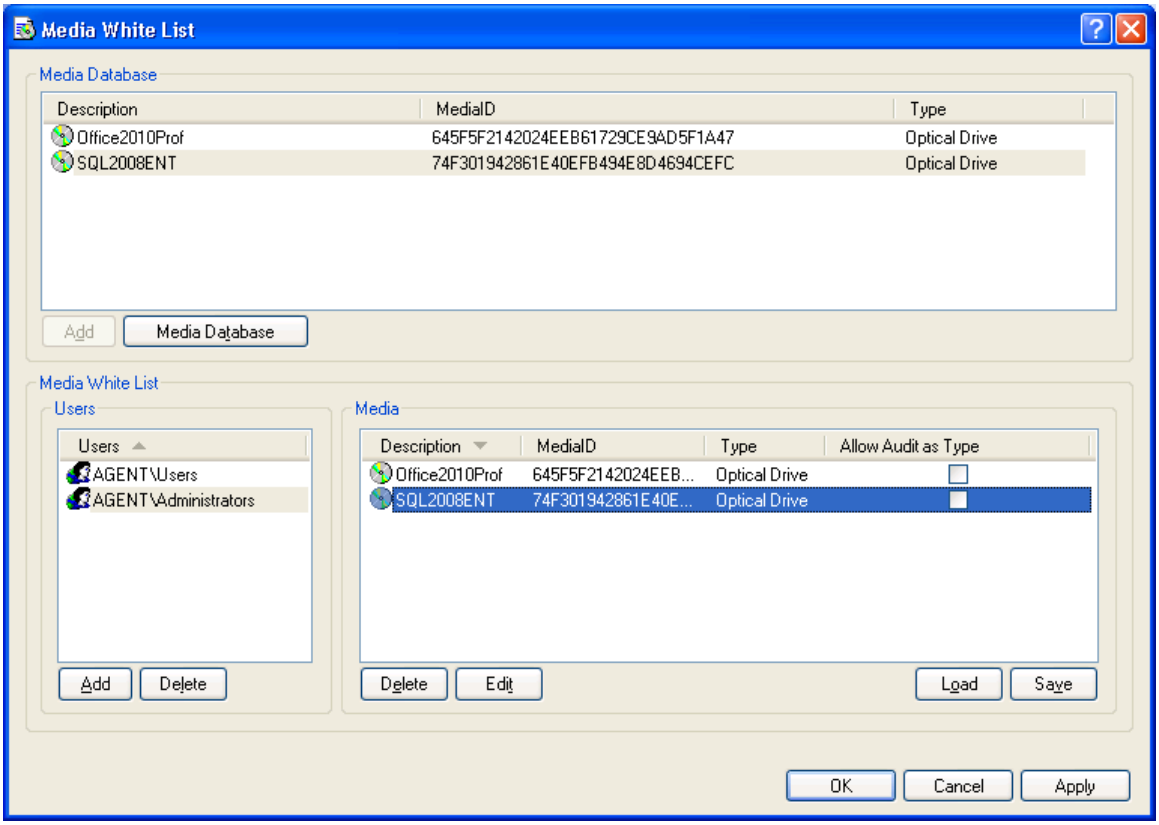
Note: Access to white listed media can be granted only on the type (Optical Drive) level. If the CD/DVD/BD drive plugs into the port (USB or FireWire) and access to this port is denied, then access to the white listed media is denied too.

Two steps are required to authorize media:

1. Add the media to the media database, making it available for adding to the white list.
2. Add the media to the white list for the specified user/group. In effect, this designates the media as authorized and allows it (read access) for this user/group at the type (Optical Drive) level.

Note: You can define different online vs. offline Media White Lists for the same user or sets of users. The online Media White List (Regular Profile) applies to client computers that are working online. The offline Media White List (Offline Profile) applies to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define the offline Media White List, see "Managing Offline Media White List."

To define the online (regular) media white list, select **Manage** from the context menu available with a right mouse click. Alternatively, you can press the appropriate button on the toolbar.



In the **Media Database** list at the top of the dialog box, you can see all media that were added to the database.

Once media are added from the database to the white list of a certain user, they become authorized media for which access control is disabled when this user is logged in.

You can add media to the Media White List in two steps:

1. Select a user or user group for which this media should be allowed. Click **Add** under the **Users** list to add the user/group. To delete the record from the **Users** list, click **Delete**.
2. Select the appropriate media record in the **Media Database** list and click **Add**.

To enable auditing and alerting for the white listed media according to settings defined in Auditing, Shadowing & Alerts (for the Optical Drive device type), select the **Allow Audit as Type** check box.

To edit a media's description, select the appropriate record in **Media White List** and click **Edit**. Click **Delete** to delete a selected media's record (use CTRL and/or SHIFT to select several records simultaneously).

To save the media white list to an external file, click **Save**, then select the name of the file.

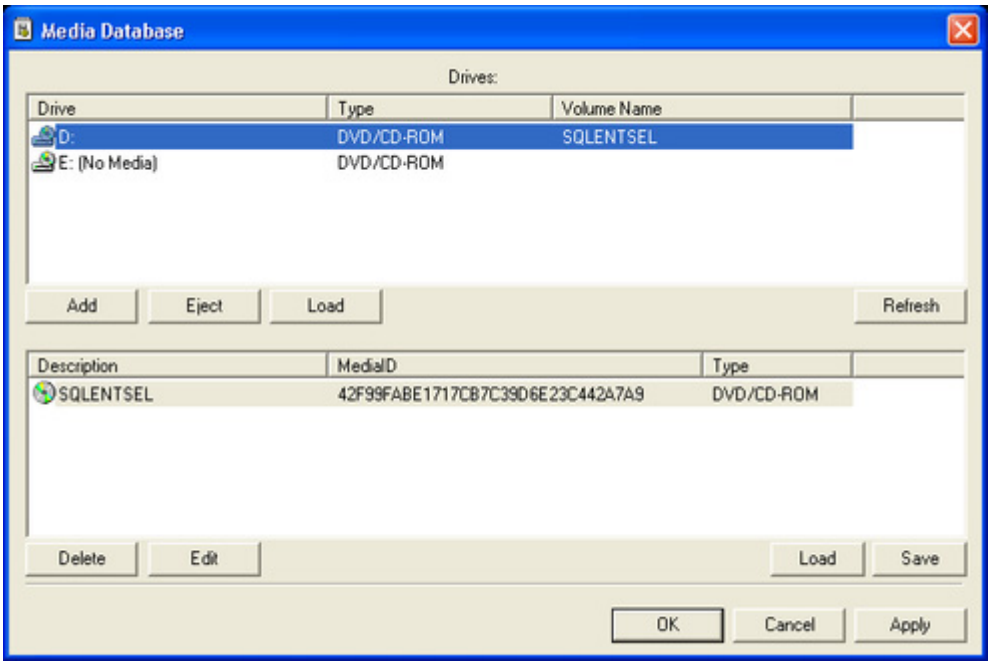
To load a previously saved white list, click **Load** and select a file that contains the list of medias.

If you need to manage the media database, you can click **Media Database** and open the appropriate dialog box.

Note: Using the media white list you can only allow read access to authorized media. It is impossible to authorize media for writing.

Media Database

In the **Media Database** dialog box you can add new media to the database and edit existing records.



Before the media can be authorized in the white list, it must be added to the database.

In the **Drives** list at the top of the dialog box, you can see all drives available on the local computer that can contain medias.

The list is automatically refreshed and displays new medias as soon as they arrive. To manually refresh this list, click **Refresh**.

In the list at the bottom of the dialog box, you can see media that are already in the database.

You can add media to this list by selecting the desired record in the **Drives** list and clicking **Add**. It takes some time (depending on the media size) to authorize the media. If the media is already in the database, it cannot be added there a second time.

To edit a media description, select the appropriate record in the list and click **Edit**.

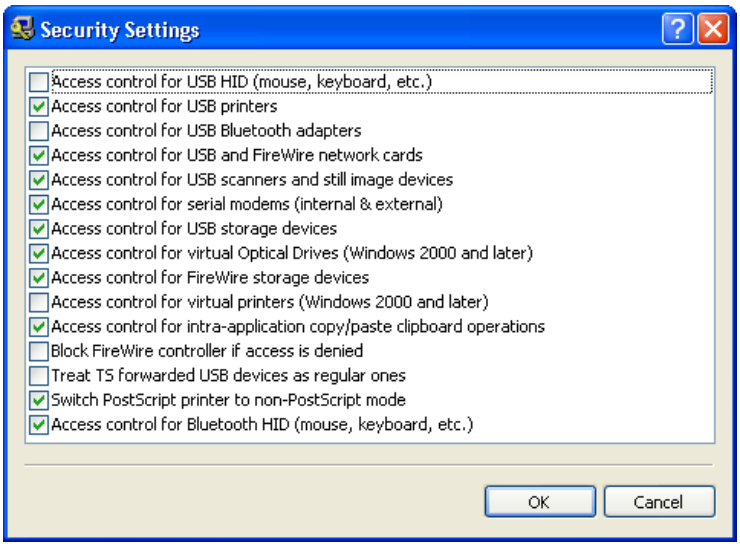
Click **Delete** to delete a selected record (use CTRL and/or SHIFT to select several records simultaneously).

You can also save a current database to an external file. To save the database to an external file, click **Save**, then select the type of the file — .txt or .csv.

To load a previously saved database, click **Load** and select a file that contains the list of medias.

Security Settings (Regular Profile)

There is a list of additional security parameters that affect permissions and audit rules for some device types.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB Bluetooth adapters
Access control for USB and FireWire network cards
Access control for USB scanners and still image devices
Access control for serial modems (internal & external)
Access control for USB storage devices
Access control for virtual Optical Drives (Windows 2000 and later)
Access control for FireWire storage devices
Access control for virtual printers (Windows 2000 and later)
Access control for intra-application copy/paste clipboard operations
Block FireWire controller if access is denied
Treat TS forwarded USB devices as regular ones
Switch PostScript printer to non-PostScript mode
Access control for Bluetooth HID (mouse, keyboard, etc.)
OK
Cancel

These security parameters enable you to keep some device types completely locked, but allow the use of certain device classes without need to authorize every device in the white list.

For example, you can disallow using all USB devices except any mouse and keyboard devices that connect through the USB.

DeviceLock supports these additional security parameters:

- **Access control for USB HID** – if enabled, allows DeviceLock Service to audit and control access to Human Interface Devices (mouse, keyboard, and so on) plugged into the USB port. Otherwise, even if the USB port is locked, Human Interface Devices continue to function as usual and audit is not performed for these devices.
- **Access control for USB printers** – if enabled, allows DeviceLock Service to audit and control access to printers plugged into the USB port. Otherwise, even if the USB port is locked, printers continue to function as usual and audit is not performed for these devices.
- **Access control for USB scanners and still image devices** – if enabled, allows DeviceLock Service to audit and control access to scanners and still image devices plugged into the USB port. Otherwise, even if the USB port is locked, these devices continue to function as usual and audit is not performed for these devices.
- **Access control for USB Bluetooth adapters** – if enabled, allows DeviceLock Service to audit and control access to Bluetooth adapters plugged into the USB port. Otherwise, even if the USB port is locked, Bluetooth adapters continue to function as usual and audit is not performed for these devices.

  This parameter affects audit and access control on the interface (USB) level only. If the device belongs to both levels, the permissions and audit rules (if any) for the type (Bluetooth) level will be applied anyway.

- **Access control for USB storage devices** – if enabled, allows DeviceLock Service to audit and control access to storage devices (such as flash drives) plugged into the USB port. Otherwise, even if the USB port is locked, storage devices continue to function as usual and audit is not performed for these devices.

  This parameter affects audit and access control on the interface (USB) level only. If the device belongs to both levels: interface and type, the permissions and audit rules (if any) for the type (Removable, Floppy, Optical Drive or Hard disk) level will be applied anyway.

- **Access control for USB and FireWire network cards** – if enabled, allows DeviceLock Service to audit and control access to network cards plugged into the USB or FireWire (IEEE 1394) port. Otherwise, even if the USB or FireWire port is locked, network cards continue to function as usual and audit is not performed for these devices.
- **Access control for FireWire storage devices** – if enabled, allows DeviceLock Service to audit and control access to storage devices plugged into the FireWire port. Otherwise, even if the FireWire port is locked, storage devices continue to function as usual and audit is not performed for these devices.

  This parameter affects audit and access control on the interface (FireWire) level only. If the device belongs to both levels: interface and type, the permissions and audit rules (if any) for the type (Removable, Floppy, Optical Drive or Hard disk) level will be applied anyway.

- **Access control for serial modems (internal & external)** – if enabled, allows DeviceLock Service to audit and control access to modems plugged into the COM port. Otherwise, even if the COM port is locked, modems continue to function as usual and audit is not performed for these devices.
- **Access control for virtual Optical Drives** – if enabled, allows DeviceLock Service to audit and control access to virtual (software emulated) CD/DVD/BD-ROMs. Otherwise, even if the CD/DVD/BD device is locked, virtual drives continue to function as usual and audit is not performed for these devices. This parameter is effective only for Windows 2000 and later systems.
- **Access control for virtual printers** – if enabled, allows DeviceLock Service to audit and control access to virtual printers which do not send documents to real devices, but instead print to files (for example, PDF converters). Otherwise, even if the physical printer is locked, virtual printers continue to print as usual and audit is not performed for them. This parameter is effective only for Windows 2000 and later systems.
- **Access control for intra-application copy/paste clipboard operations** – if enabled, allows DeviceLock Service to audit and control access to copy/paste operations within an application. Otherwise, even if the clipboard is locked, access control for copy/paste operations within one application is disabled and audit is not performed for them.
- **Block FireWire controller if access is denied** – if enabled, allows DeviceLock Service to disable FireWire controllers when the Everyone account has No Access permissions for the FireWire port device type.
- **Switch PostScript printer to non-PostScript mode** – if enabled, DeviceLock Service makes PostScript printers act like non-PostScript printers. This resolves an issue in which DeviceLock Service is unable to create a correct shadow copy of printed data and perform content analysis of data sent to printers that use a PostScript driver.
- **Treat TS forwarded USB devices as regular ones** – if enabled, allows DeviceLock Service to control access to all USB devices redirected during a Citrix XenDesktop/MS RemoteFX session according to the rights set for the USB port device type. Otherwise, DeviceLock Service controls access to all USB devices redirected during a Citrix XenDesktop/MS RemoteFX session according to the **USB Devices Access** right set for TS Devices.
- **Access control for Bluetooth HID** – if enabled, allows DeviceLock Service to audit and control access to Human Interface Devices (mouse, keyboard, and so on) connected via Bluetooth. Otherwise, even if Bluetooth is locked, Human Interface Devices continue to function as usual and audit is not performed for these devices.

  This parameter affects audit and access control on the type (Bluetooth) level only. If the device belongs to both levels: interface and type, the permissions and audit rules (if any) for the interface (USB) level will be applied anyway.

Note: You can define different online vs. offline Security Settings for the same user or sets of users. Online Security Settings (Regular Profile) apply to client computers that are working online. Offline Security Settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define offline Security Settings, see "Managing Offline Security Settings."

To change online (regular) security parameters, double-click the parameter's record to switch its state (**enable**/**disable**). Alternatively, you can select **Manage** from the context menu available with a right mouse click or press the appropriate button on the toolbar.

Security Settings are similar to the device white list but there are three major differences:

1. Using Security Settings you can only allow a whole class of device. You cannot allow only a specific device model, while locking out all other devices of the same class.

   For example, by disabling **Access control for USB storage devices**, you allow the use of all USB storage devices, no matter their model and vendor. By specifying the one USB Flash Drive model you want to allow on the devices white list, you ensure that all other USB storage devices remain locked out.

2. Using Security Settings you can only select from the predefined device classes. If the device does not belong to one of the predefined classes, then it cannot be allowed.

   For example, there is no specific class for smart card readers in Security Settings, so if you want to allow a smart card reader when the port is locked, you should use the devices white list.

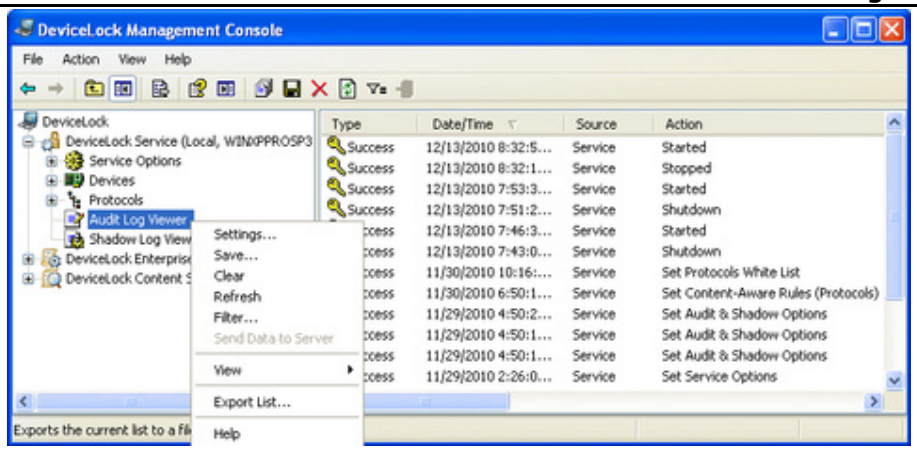
3. Security Settings cannot be defined on a per-user basis; they affect all users of the local computer. However, devices in the white list can be defined individually for the every user and group.

Note: Security Settings work only for those devices that are using standard Windows drivers. Some devices are using proprietary drivers and their classes cannot be recognized by DeviceLock Service. Hence, access control to such devices cannot be disabled via Security Settings. In this case you may use the devices white list to authorize such devices individually.

Audit Log Viewer (Service)

There is a built-in audit log viewer that allows you to retrieve DeviceLock audit log records from a computer's local Windows event logging subsystem.

The standard Windows event logging subsystem is used to store audit records, only if **Event Log** or **Event & DeviceLock Logs** is selected in the **Audit log type** parameter in Service Options. Otherwise, audit records are stored in the proprietary log and can be viewed using the server's audit log viewer.



The audit log stores events generated by a user's device-related activities that fall under the audit rules. For more information, please read the Auditing, Shadowing & Alerts section of this manual.

Also, changes in a DeviceLock Service's configuration generate events in the audit log, if the appropriate check box is selected in Service Options.

The columns of this viewer are defined as follows:

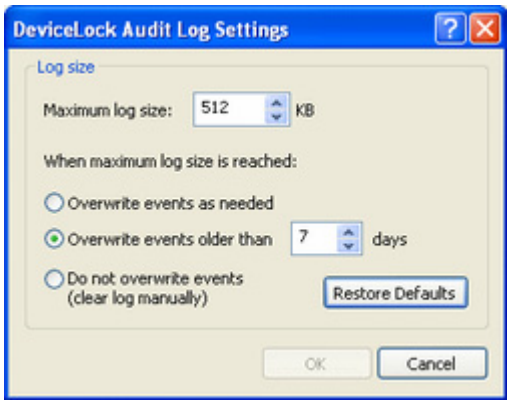
- **Type** – the class of an event, either **Success** for allowed access or **Failure** for denied access.
- **Date/Time** – the date and the time when an event was received by DeviceLock Service.
- **Source** – the type of device or protocol involved.
- **Action** – the user's activity type.
- **Name** – the name of the object (file, USB device, etc.).
- **Information** – other device-specific information for the event, such as the access flags, devices names, and so on.
- **Reason** - the cause of the event. Possible reasons include: **Content-Aware Rule error**, **Device Permissions**, **IP Firewall**, **Passthru**, **Protocol Permissions**, **Rule**, **Security Settings**, **Shadowing error**, **White List**, **Local Storage Quota Exceeded**.
- **User** – the name of the user associated with this event.
- **PID** – the identifier of the process associated with this event.
- **Process** – the fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path.

To refresh the list of events, select **Refresh** from the context menu available by a right mouse click or press the appropriate button on the toolbar.

To clear all events from the audit log, select **Clear** from the context menu or press the appropriate button on the toolbar.

Audit Log Settings (Service)

To define a maximum log size and what Windows should do if the audit log becomes full, use **Settings** from the context menu of **Audit Log Viewer** or press the appropriate button on the toolbar.



In the **Maximum log size** parameter, you can specify the maximum size of the log file (in kilobytes). The log file is created and used only by the Windows Event Log service. This file is usually located in the ***%SystemRoot%\system32\config*** directory and has the ***DeviceLo.evt*** name.

To specify what Windows should do when an event log is full (when Maximum log size is reached) select one of these options:

- **Overwrite events as needed** – the system will overwrite old events if Maximum log size is reached.
- **Overwrite events older than** – specifies that records that are newer than this value will not be overwritten (specified in days).
- **Do not overwrite events (clear log manually)** – the system will not overwrite old events if Maximum log size is reached and you will need to clear events manually.

Note: When the event log is full and there are no records that Windows can overwrite, then DeviceLock Service is unable to write new audit records to this log.

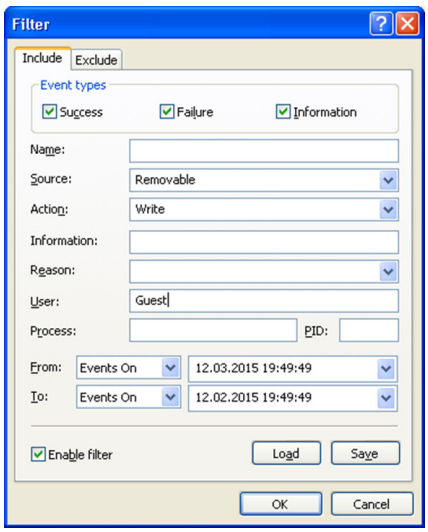
If you wish to reset current settings to the default values, click **Restore Defaults**. Default values are:

- The **Maximum log size** parameter is set to 512 kilobytes.
- The **Overwrite events older than** option is selected and set to 7 days.

Audit Log Filter (Service)

You can filter data in Audit Log Viewer so that only records that meet specific conditions are displayed in the list.

To open the **Filter** dialog box, use **Filter** from the context menu of **Audit Log Viewer** or press the appropriate button on the toolbar.



There are two types of filters:

- **Include** – only entries that match conditions specified on the **Include** tab are shown in the list.
- **Exclude** – entries that match conditions specified on the **Exclude** tab are not shown in the list.

To use any filter, you should activate it first. Select the **Enable filter** check box to make a filter active. To temporary deactivate the filter, clear the **Enable filter** check box.

When the filter is active you can define its condition by entering values into the following fields:

- **Success audit** – specifies whether to filter device access attempts that were successful.
- **Failure audit** – specifies whether to filter device access attempts that failed.
- **Information audit** – specifies whether to filter attempts to transfer data content monitored by Content-Aware rules of "Detection" type.
- **Name** – the text that matches a value in the Audit Log Viewer's **Name** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Source** – the text that matches a value in the Audit Log Viewer's **Source** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Action** – the text that matches a value in the Audit Log Viewer's **Action** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).

- **Information** – the text that matches a value in the Audit Log Viewer's **Information** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Reason** - the text that matches a value in the Audit Log Viewer's **Reason** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **User** – the text that matches a value in the Audit Log Viewer's **User** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Process** – the text that matches a value in the Audit Log Viewer's **Process** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **PID** – the number that matches a value in the Audit Log Viewer's **PID** column.
  You can enter multiple values separated by a semicolon (;).
- **From** – specifies the beginning of the interval of events that you want to filter. Select **First Event** to see events starting with the first event recorded in the log. Select **Events On** to see events that occurred starting with a specific time and date.
- **To** – specifies the end of the range of events that you want to filter. Select **Last Event** to see events ending with the last event recorded in the log. Select **Events On** to see events that occurred ending with a specific time and date.

The AND logic is applied to all specified fields and between active filters (Include/Exclude). It means that the filter's result includes only those records that comply with all defined conditions.

If you do not want to include a field to the filter's condition, just leave this field empty.

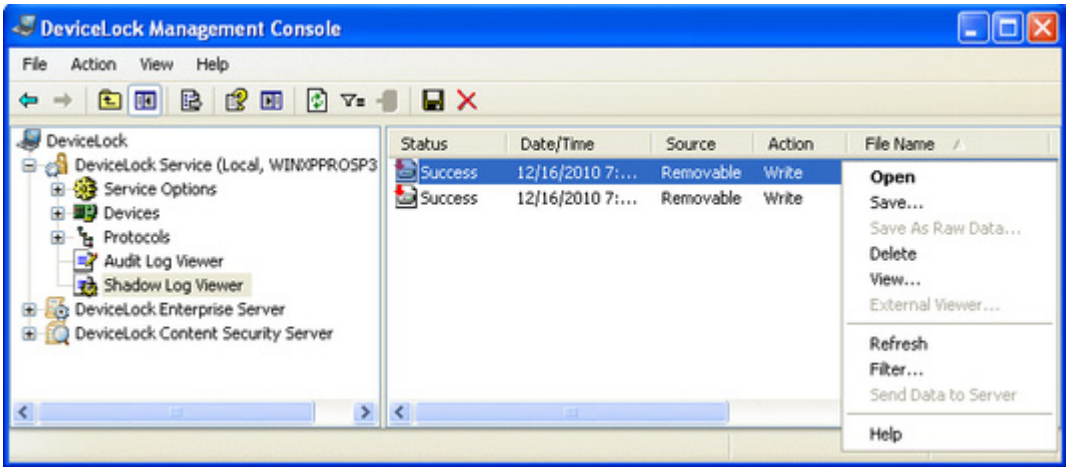
For some fields you can use wildcards. A wildcard is a character such as an asterisk (*) or a question mark (?) that is used to represent one or more characters when you are defining a filter.

Use the asterisk as a substitute for zero or more characters. If you are looking for a name that you know starts with "win" but you cannot remember the rest of the name, type the following: **win***. This locates all names that begin with "win" including Windows, Winner, and Wind.

Use the question mark as a substitute for a single character in a name. For example, if you type **win?**, you will locate Wind but not Windows or Winner.

Shadow Log Viewer (Service)

There is a built-in shadow log viewer that allows you to retrieve the shadow log from DeviceLock Service.



The typical DeviceLock configuration assumes that the shadow data is stored on DeviceLock Enterprise Server. In this case all shadow data which is originally logged and cached by DeviceLock Service on the local computer is periodically moved to the server. The local shadow log is cleared as soon as the data is successfully moved to the server, so to view this data, you should use the server's shadow log viewer.

However, in some cases you may need to view the shadow log of a certain computer. This need arises when, for example, you do not use DeviceLock Enterprise Server at all or when the server is being used, but for some reason the data still exists on the client computer.

The columns of this viewer are defined as follows:

- **Status** – indicates the status of the record. The **Success** status indicates that data is successfully logged; the **Incomplete** status indicates that data is possibly not completely logged while the **Failed** status is given to shadow copies of files checked by Content-Aware Rules and whose transmission was blocked.
- **Date/Time** – the date and the time when the data was transferred.
- **Source** – the type of device or protocol involved.
- **Action** – the user's activity type.
- **File Name** – the original path to the file or the auto-generated name of the data that originally was not a file (such as CD/DVD/BD images, data written directly to the media or transferred through the serial/parallel ports).
- **File Size** – the size of the data.
- **File Type** – the real file type of the file.

> **Note:** When applied to files that have been transferred to Removable, Floppy, or Optical drive devices, this column is empty until a device or a disc the files were transferred to, are unplugged/removed.

- **Protected** – indicates the protection status of a file. **Yes** status indicates that the file is protected. **No** status indicates that the file is not protected. Empty status indicates that the file is not protected, and does not have protection features. **Error** <text> status indicates an error during protection status detection has occurred.

  Note: Protection status can only be retrieved on Windows XP or later operating systems. Retrieval attempts made on older operating systems return the "unsupported system" error that can be found in Server- and Audit Log Viewer.

- **User** – the name of the user transferred the data.
- **PID** – the identifier of the process used to transfer the data.
- **Process** – fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path.

Use the context menu available via a right mouse click on every record.

Open
To open the file from a selected record with its associated application, use **Open** from the context menu. If there is no associated application then the **Open With** dialog box is shown. In case the record has no associated data (its size is 0 or it was not logged), **Open** is disabled.

If you use **Open** for shadowing data captured from the Parallel port device type then the associated application is always the built-in viewer called DeviceLock Printer Viewer.

DeviceLock Printer Viewer is able to show you the shadowed printed document in the PostScript and native print spooler format, send it to the printer again, or save it as a graphic file (such as BMP, GIF, JPEG, PNG, EMF or TIFF). Next print spooler formats are supported: PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, GDI printing (ZjStream) and EMF Spooled Files.

To enable EFS encryption of temporary files created when a shadow copy is opened/viewed, open **Regedit** and set the following entry:

- Key: **HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision**
- Name: **EncryptTempFiles**
- Type: **DWORD**
- Value: *00000001*

  Applicable values are *1=Enabled, 0=Disabled*. The default value is *0*.

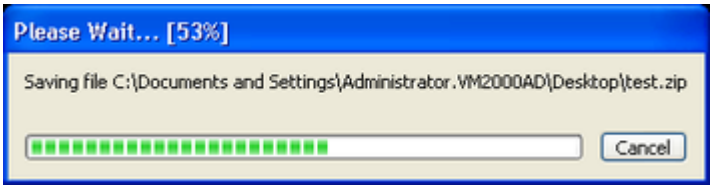
Save

If you need to save data from a selected record to your local computer, use **Save** from the context menu or press the appropriate button on the toolbar.

Use CTRL and/or SHIFT to select and save the data from several records simultaneously.

In case the record has no associated data (its size is 0 or it was not logged), **Save** is disabled in the context menu and on the toolbar.

The progress bar appears when you are saving a large file.



You can click **Cancel** at any time to abort the saving process. In this case the resultant file on the local computer will be incomplete and will contain only that part of the data which was received before you aborted the saving process.

If the data was transferred by the user as a file, it is stored in the shadow log as a file and can be saved to the local computer as a file too.

When a user has written data to a CD/DVD/BD disk, all data is stored in a shadow log as a single CD/DVD/BD image (one image per each written CD/DVD/BD disk or session) in the CUE format.

CD/DVD/BD images as well as other data that originally was not transferred as files (direct media access or serial/parallel ports transfer) have auto-generated names based on the action's type, drive's letter or device's name and time/date (for example, direct_write(E:) 19:18:29 17.07.2006.bin).

Each CD/DVD/BD image is saved to the local computer as two files: the data file with the .bin extension (for example, direct_write(E_) 19_18_29 17_07_2006.bin) and the cue sheet file that has the same name as its data file with the .cue extension (for example, direct_write(E_) 19_18_29 17_07_2006_bin.cue). These both files are necessary to open the CD/DVD/BD image in the external application that supports the CUE format (such as Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO and many others).

Save As Raw Data

When you select a record that contains the data originally written as an additional session to a multi-session CD/DVD/BD disk, the **Save As Raw Data** item is available in the context menu. It allows you to save the data to the local computer as is (without fixing references to the data in previous sessions).

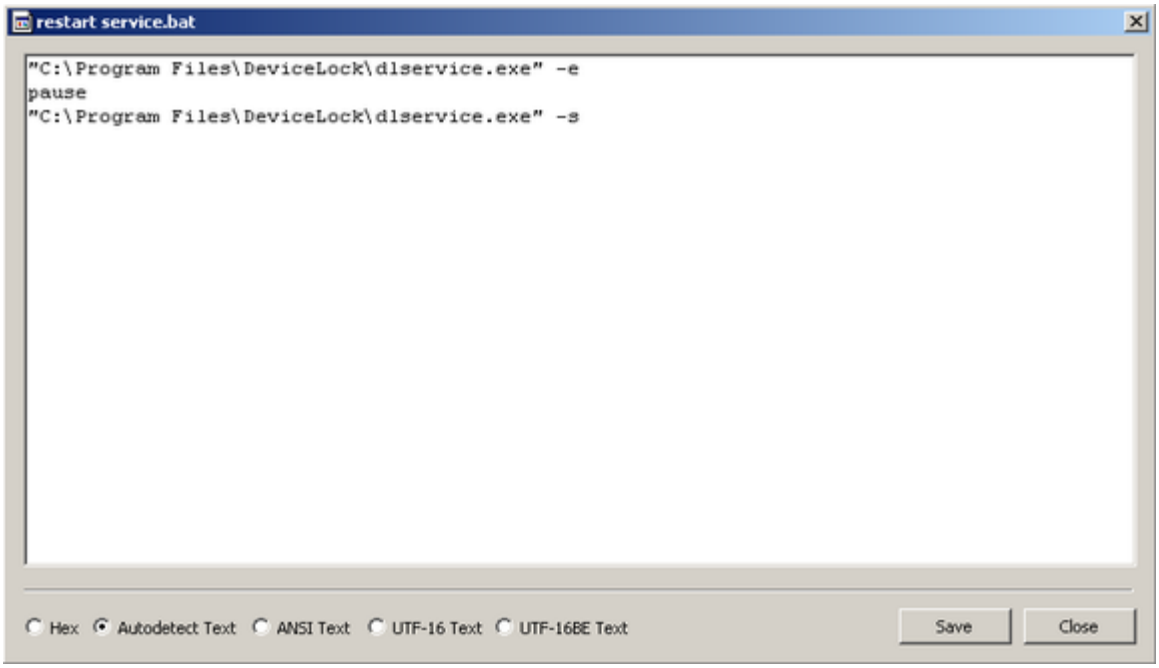
If you are using the regular saving function (the **Save** command or the toolbar's button), DeviceLock Management Console detects that the CD/DVD/BD image contains a session that refers to the data in other (previous) sessions. Since the previous sessions are not available (they could be written on the computer where DeviceLock Service is not installed), DeviceLock Management Console locates and fixes all references to these non-existent sessions to make the .cue file readable by applications that support this format.

However, if you need to get the data that was not modified by DeviceLock Management Console, use **Save As Raw Data**. In this case the resultant file may be unreadable by applications that support the CUE format.

When saving large files, you can click the **Cancel** button on the progress bar to abort the saving process. In this case the resultant file on the local computer will contain only that part of the data which was received before you aborted the saving process.

View

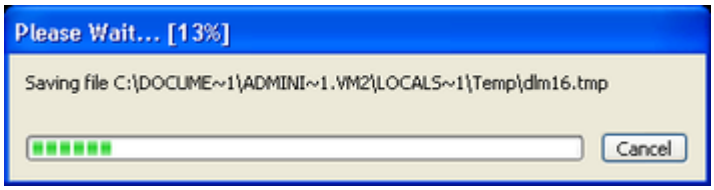
To open the data in the built-in viewer, use **View** from the context menu.



In the built-in viewer, click any of the following viewing options:

- **Hex** Displays data in hex as well as in words.
- **Autodetect Text** Enables the auto-detection of encoding for text and displays data in textual format only.
- **ANSI Text** Specifies ANSI encoding for text and displays data in textual format only.
- **UTF-16 Text** Specifies Unicode UTF-16 encoding for text and displays data in textual format only.
- **UTF-16BE Text** Specifies Unicode UTF-16 (Big Endian) encoding for text and displays data in textual format only.

When you are opening the large file, you can click **Cancel** on the progress bar to abort the opening process.



In this case the viewer will show only that part of the data which was received before you aborted the opening process.

Click **Save** to save the data from the viewer to an external file.

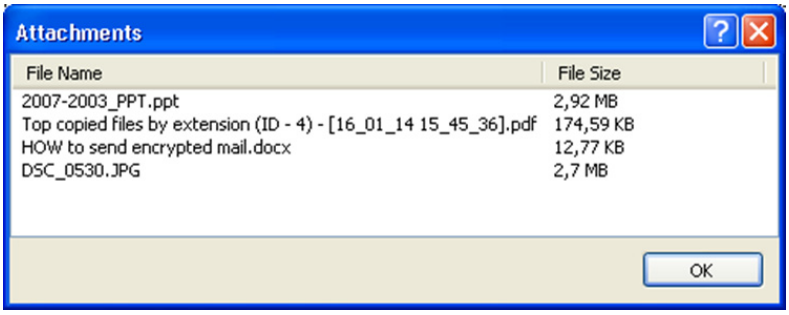
External Viewer
Also, you can define the external program that will be used to view the shadow data.

If such an external application is defined, **External Viewer** is available on the shortcut menu. To define it, open **Regedit** and set the following entry on the computer where DeviceLock Management Console is running:

- Key: **HKEY_CURRENT_USER\Software\SmartLine Vision\DLManager\Manager**
- Name: **ExternalShadowViewer**
- Type: **REG_SZ**
- Value: *<full_path_to_viewer>* **%1**
  where *<full_path_to_viewer>* must be replaced by the full path to the external application. If this path contains spaces, use quotation marks. For example: "C:\Program Files\Microsoft Office\OFFICE11\winword.exe" %1.

When you are opening a large file, you can click **Cancel** on the progress bar to abort the opening process. In this case the external application will receive only that part of the data which was received before you aborted the opening process.

View Attachments
For .eml shadow copies of messages sent/received via SMTP, Web Mail, IBM Notes, or MAPI protocols, you can view attachments (if any).



Delete
To delete a record, select **Delete** from the context menu or press the appropriate button. Use CTRL and/or SHIFT to select and remove several records simultaneously.

Refresh
To refresh the list, select **Refresh** from the context menu available via a right mouse click or press the appropriate button on the toolbar.

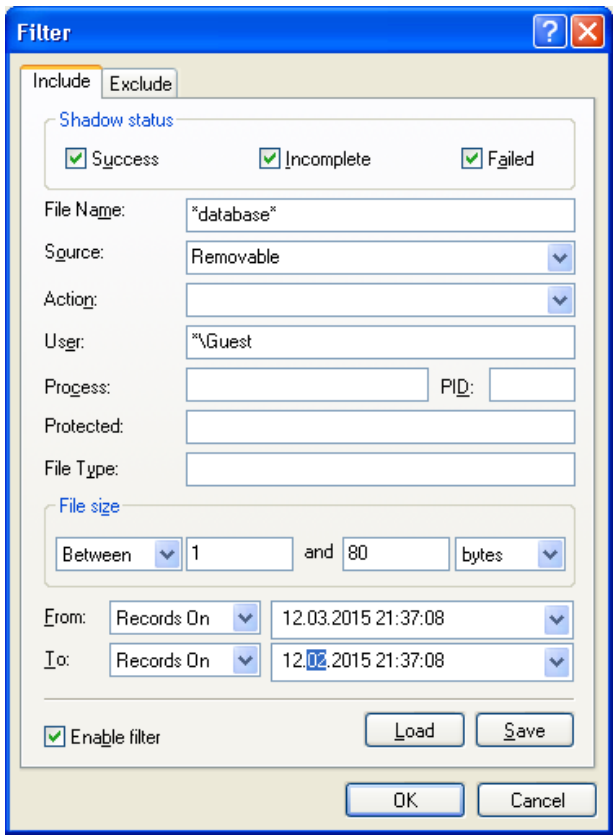
Send Data to Server

When DeviceLock Enterprise Server is defined in Service Options and you need to force moving the shadow data from the current computer to the server, use **Send Data to Server** from the context menu available by a right mouse click or press the appropriate button on the toolbar.

Shadow Log Filter (Service)

You can filter data in Shadow Log Viewer so that only records that meet certain conditions are displayed in the list.

To open the **Filter** dialog box, use **Filter** from the context menu of **Shadow Log Viewer** or press the appropriate button on the toolbar.



There is no big difference between defining Audit Log Filter and Shadow Log Filter, so first read the Audit Log Filter (Service) section of this manual.

When the filter is active you can define its condition by entering values into the following fields:

- **Success** – specifies whether to filter the successfully logged data.
- **Incomplete** – specifies whether to filter the data that was logged incompletely.

- **Failed** – specifies whether to filter the logged data checked by Content-Aware Rules and whose transmission was blocked.
- **File Name** – the text that matches a value in the Shadow Log Viewer's **File Name** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Source** – the selection that matches a value in the Shadow Log Viewer's **Source** column.
  You can enter multiple values separated by a semicolon (;).
- **Action** – the selection that matches a value in the Shadow Log Viewer's **Action** column.
  You can enter multiple values separated by a semicolon (;).
- **User** – the text that matches a value in the Shadow Log Viewer's **User** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Process** – the text that matches a value in the Shadow Log Viewer's **Process** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **PID** – the number that matches a value in the Shadow Log Viewer's **PID** column.
  You can enter multiple values separated by a semicolon (;).
- **Protected** – the text that matches a value in the Shadow Log Viewer's **Protected** column.
- **File Type** – the text that matches a value in the Shadow Log's Viewer **File Type** column. This text is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **File size** – the number or the region of numbers that matches a value in the Shadow Log Viewer's **File Size** column.
- **From** – specifies the beginning of the interval of records that you want to filter. Select **First Record** to see records starting with the first record written to the log. Select **Records On** to see records that were written starting with a specific time and date.
- **To** – specifies the end of the range of records that you want to filter. Select **Last Record** to see records ending with the last record written to the log. Select **Records On** to see records that were written ending with a specific time and date.

Managing DeviceLock Service for Mac

DeviceLock Service for Mac can be managed via DeviceLock Management Console in much the same way as you manage DeviceLock Service for Windows.

Note: To allow remote management via DeviceLock management consoles using local user credentials for machine where DeviceLock Service for Mac was installed, the **Share File and Folders using SMB (Windows)** system option must be enabled for these local users or the NTLM hashes must be enabled for these accounts. For more information on this, see "Enabling NTLM authentication for local users on Mac OS X".

In comparison to DeviceLock Service for Windows, DeviceLock Service for Mac supports only these settings and parameters:

Service Options

- DeviceLock Administrators (unsupported parameters: *Enable Unhook Protection*, *Prevent Changes in System Configuration Files*, *Use Strong Integrity Check*)
- DeviceLock Enterprise Server(s)
- DeviceLock Certificate
- Use Group Policy
- Fast server first
- Offline mode detection
- Override Local Policy
- Log policy changes and Start/Stop events

Service Options -> Auditing & Shadowing

- Transfer shadow data to server

Service Options -> Encryption

- Mac OS X FileVault

Devices

- Bluetooth (Permissions, Audit)
- FireWire port (Permissions, Audit)
- Hard disk (Permissions, Audit)
- Optical Drive (Permissions, Audit)
- Removable (Permissions, Audit, Shadowing)
- Serial port (Permissions, Audit)
- USB port (Permissions, Audit)
- WiFi (Permissions, Audit)
- USB White List (the only flag supported is *Control as type*)
- Media White List

Note: Bluetooth permissions are not applied to Bluetooth HID devices, so access to the devices is always allowed to prevent wireless HID devices (mice and keyboards) from being disabled on iMac and Mac Pro hardware.

Security Settings

- Access control for USB HID
- Access control for USB Bluetooth adapters
- Access control for USB and FireWire network cards
- Access control for USB storage devices
- Access control for FireWire storage devices

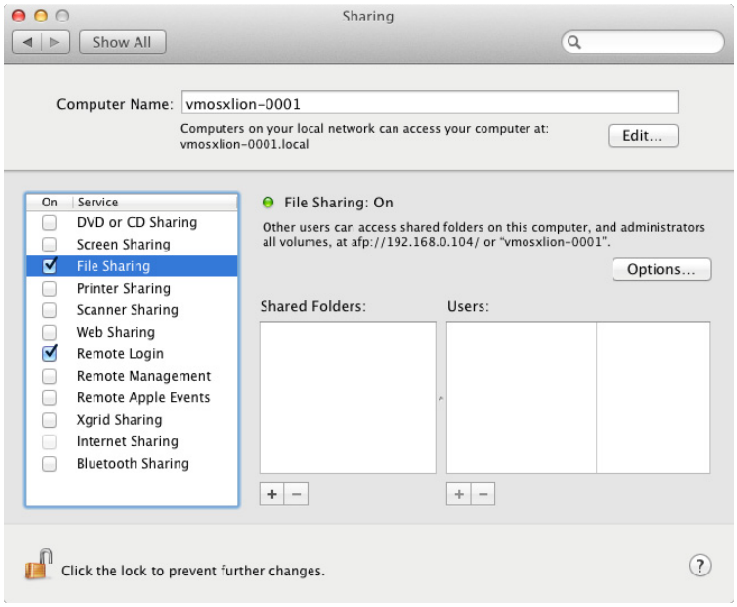
Enabling NTLM authentication for local users on Mac OS X

The DeviceLock Service for Mac employs NTLM authentication and encryption in order to secure network communications with other DeviceLock components. If the Mac computer is integrated in Active Directory authentication with a domain account, it will just work. However, NTLM authentication with local users is normally disabled. In order to manage a standalone Mac with DeviceLock management consoles, NTLM authentication MUST be enabled for the local user.

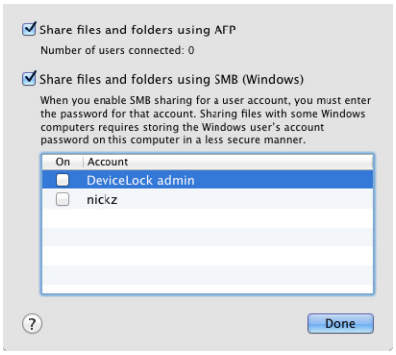
There are two ways to enable NTLM for a local user on Mac:

1. **The user-friendly way.** This method works for Mac OS X 10.7 and later. See below for the 10.6 method.

   Navigate to **Sharing** pane in System Preferences, and select **File Sharing**.



   Click **Options**.


Share files and folders using AFP
Number of users connected: 0
Share files and folders using SMB (Windows)
When you enable SMB sharing for a user account, you must enter the password for that account. Sharing files with some Windows computers requires storing the Windows user's account password on this computer in a less secure manner.
On
Account
DeviceLock admin
nickz
Done

Below **Share files and folder using SMB (Windows)** is the list of all local users. Enabling Windows file sharing on a local account turns on the support for NTLM authentication.

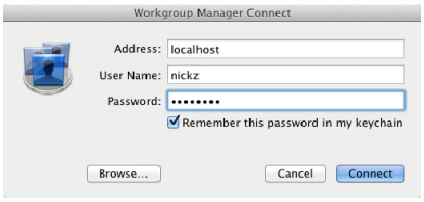
Note: The support for NTLM authentication is enabled on per-user basis.

2. **The alternate way.** This method works for Mac OS X 10.6, 10.7 and later.

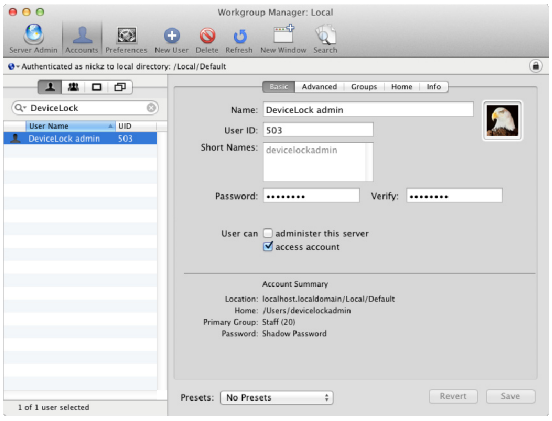
   Install Server Admin Tools:

   - Server Admin Tools 10.6.8 http://support.apple.com/kb/HT3931
   - Server Admin Tools 10.7.3 http://support.apple.com/kb/HT202366

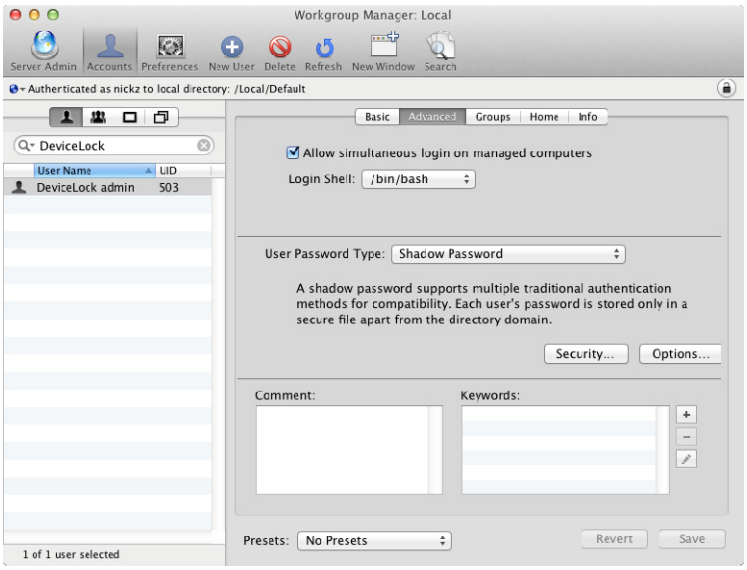
   Launch Workgroup Manager from Server Admin Tools. The authentication dialog will pop up. Specify the name of a computer to connect to and provide an administrator's credentials.



After successful authentication, the main window appears. Select a user from the list to the left.



Open **Advanced** tab.



Click **Security**.

Please select authentication methods for this user account.
Hash Methods
These methods store passwords in forms more difficult for attackers to decode.
CRAM-MD5 (mail service clients)
NTLMv1 and NTLMv2 (clients using Windows NT/98 or later)
LAN Manager (Windows 95 clients)
Recoverable Authentication Methods
These methods store passwords in forms an attacker could decode after gaining direct access to the server's password database.
WebDAV-Digest and APOP (web and mail service clients)
Cancel
OK

Check **NTLMv1 and NTLMv2** option, and apply changes. Finally, change the password of the user for which NTLM authentication was enabled.

Note: NTLM authentication will not be available until the user password is changed. This is the inherent limitation of the secure password database of Mac OS X.

The new password is not required to be different from the old one.

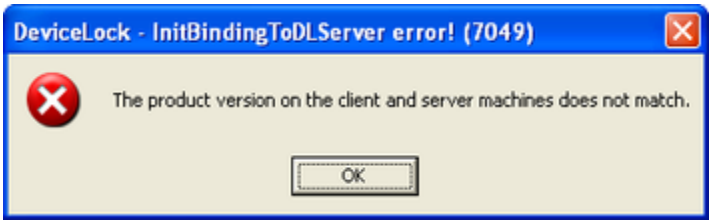
The support for NTLM authentication is enabled on per-user basis.

Managing DeviceLock Enterprise Server

Expand the **DeviceLock Enterprise Server** item to get access to all of a server's functions and configuration parameters.

There is a context menu available by a right mouse click on the **DeviceLock Enterprise Server** item:

- **Connect** – connects to any computer that you specify. For more information please read the Connecting to Computers section of this manual.
  When you connect to a computer where an old version of DeviceLock Enterprise Sever is installed, you may receive the following message.

  In this case you need to install the new version DeviceLock Enterprise Server on this computer. For information on how to install DeviceLock Enterprise Server, please read the Installing DeviceLock Enterprise Server section of this manual.

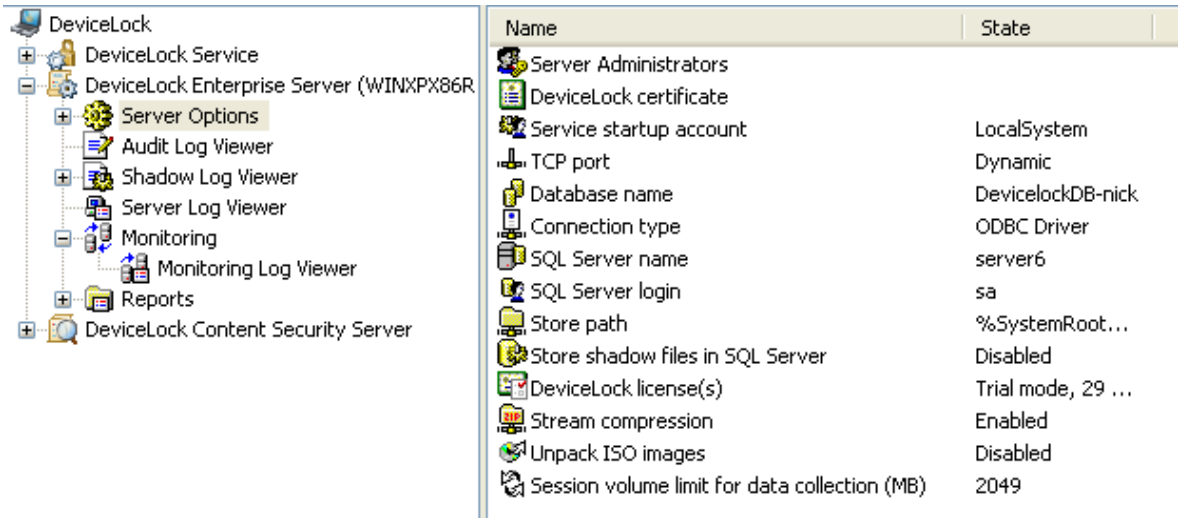
- **Reconnect** – connects to the currently connected computer once again.
- **Connect to Last Used Server at Startup** – check this flag to instruct DeviceLock Management Console to automatically connect to the last used server each time console starts up.
- **Certificate Generation Tool** – runs the special tool that allows you to generate DeviceLock Certificates. For more information please read the Generating DeviceLock Certificates section of this manual.
- **DeviceLock Signing Tool** – runs the special tool that allows you to grant users temporary access to requested devices and sign XML files with DeviceLock Service

settings. For more information please read the DeviceLock Signing Tool section of this manual.

- **About DeviceLock** – displays the dialog box with information about the DeviceLock version and your licenses.

Server Options

These parameters allow you to tune up the DeviceLock Enterprise Server configuration.



Use the context menu available by a right mouse click or double-click on the **Stream compression** parameter to enable or disable it. By enabling the **Stream compression** parameter, you instruct DeviceLock to compress audit logs and shadow data sending from DeviceLock Services to DeviceLock Enterprise Server. Doing this decreases the size of data transfers and thus reduces the network load.

By enabling the **Unpack ISO images** parameter you can instruct DeviceLock Enterprise Server to extract files from shadowed CD/DVD/BD images. If this parameter is enabled, all files are extracted from CD/DVD/BD images upon delivery to the server and stored in the database separately (one record per file). Otherwise, whole shadowed CD/DVD/BD images are stored in the database.

By enabling the **Session volume limit for data collection (MB)** parameter, you can limit the volume of data gathered from a single computer in order to potentially enhance overall collection performance when gathering data. Enabling this parameter is helpful when large amounts of data gathered from some agents prevent DeviceLock Enterprise Server from finishing the procedure for all requests in reasonable timeframes. If this parameter is enabled, the Devicelock Enterprise Server only gathers the specified amount of data (default value for the parameter is 1024 Mb), and then starts gathering data from the next agent request without terminating the previous connection or process.

Use the context menu on other parameters to open dialogs that enable making changes. Alternatively, you can double-click on the parameter to open its dialog box.

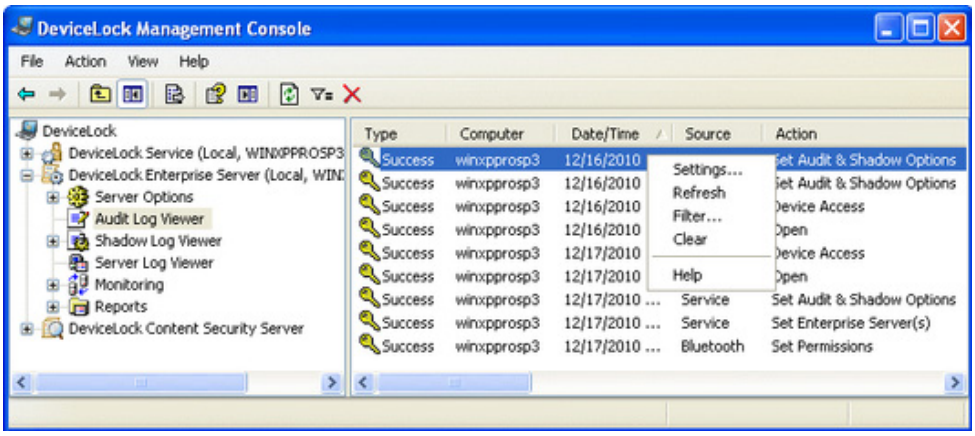
All these parameters are described in detail in the Installing DeviceLock Enterprise Server section of this manual.

To run the configuration wizard and review or set all these parameters step by step, use the **Properties** item from the context menu of **Server Options**. The configuration wizard is also described in the Installing DeviceLock Enterprise Server section of this manual.

Audit Log Viewer (Server)

The audit log viewer allows you to retrieve the audit log stored on DeviceLock Enterprise Server.

DeviceLock Enterprise Server stores audit records received from a remote computer, only if **DeviceLock Log** or **Event & DeviceLock Logs** is selected in the **Audit log type** parameter in Service Options on that computer. Otherwise, audit records are stored in the local Windows event logging subsystem of the remote computer and can be viewed using the service's audit log viewer.



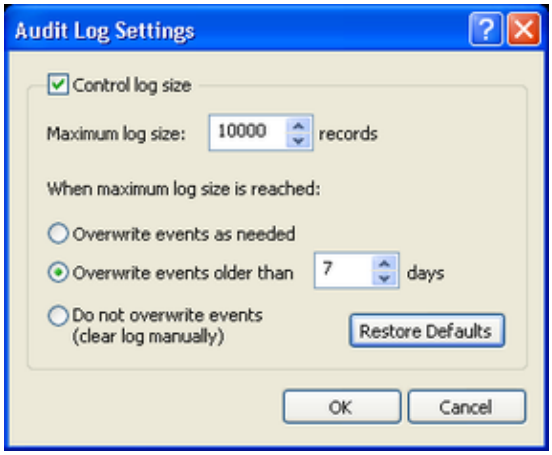
There is not much difference between the service's audit log viewer and the server's audit log viewer, so first read the Audit Log Viewer (Service) section of this manual.

In comparison with the service's audit log viewer, the server's viewer has the following additional columns:

- **Computer** – the name of the computer from which audit logs were received.
- **Event** – a number identifying the particular event type.
- **Received Date/Time** – the date and the time when an event was received by DeviceLock Enterprise Server.

Audit Log Settings (Server)

To define a maximum log size and what DeviceLock Enterprise Server should do if the audit log becomes full, use **Settings** from the context menu of **Audit Log Viewer**.



Note: These settings are stored in the database and they are specific to the log but not to DeviceLock Enterprise Server. This means that, if there are several DeviceLock Enterprise Servers using one database, all have the same log settings.

Enable the **Control log size** flag to allow DeviceLock Enterprise Server to control the number of records in the log and delete outdated records (if necessary) to clean up the space for new ones. Otherwise, if the **Control log size** flag is disabled, DeviceLock Enterprise Server uses all available space for the SQL Server's database to store the log.

In the **Maximum log size** parameter you can specify the maximum number of records that this log can contain. Please note that, if there is more than one DeviceLock Enterprise Server using this database, then the actual number of records in the log can be a little larger (by a couple of records) than the specified value.

To specify what DeviceLock Enterprise Server should do when the log is full (when Maximum log size is reached) select one of these options:

- **Overwrite events as needed** – the server will overwrite old events if Maximum log size is reached.
- **Overwrite events older than** – specifies that records that are newer than this value will not be overwritten (specified in days).
- **Do not overwrite events (clear log manually)** – the server will not overwrite old events if Maximum log size is reached and you will need to clear events manually.

Note: The actual number of records in the database may temporarily exceed the number specified in the **Maximum Log Size** parameter, since the log cleanup routine runs in the background every 30 minutes to reduce the load on the SQL Server.

If you wish to reset current settings to the default values, click **Restore Defaults**. Default values are:

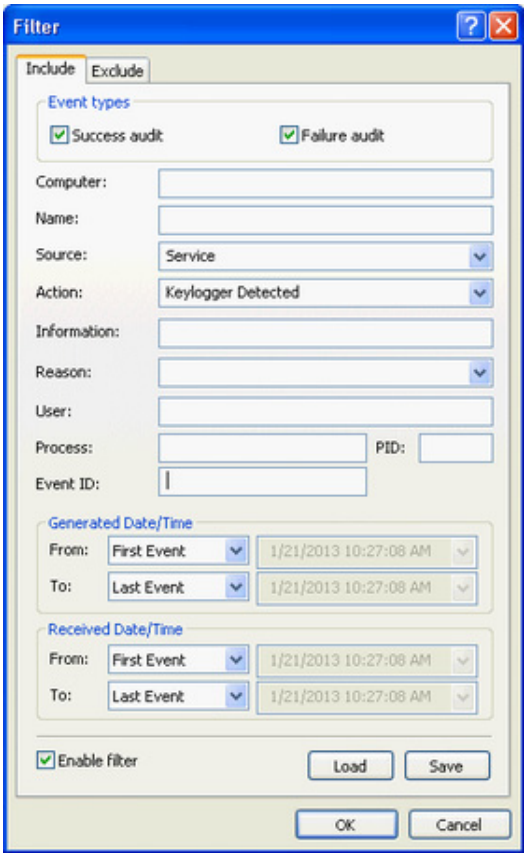
- The **Maximum log size** parameter is set to 10000 records.
- The **Overwrite events older than** option is selected and set to 7 days.

If there is no space for new records in the audit log and there is nothing to delete then DeviceLock Enterprise Server does not remove audit data from remote users' computers. This prevents you from loosing the audit data due to lack of space in the log. When some space becomes available in the log, DeviceLock Enterprise Server moves the remaining audit data from users' computers to this log.

Audit Log Filter (Server)

You can filter data in Audit Log Viewer so that only records that meet specified conditions are displayed in the list.

To open the **Filter** dialog box, use **Filter** from the context menu of **Audit Log Viewer** or press the appropriate button on the toolbar.



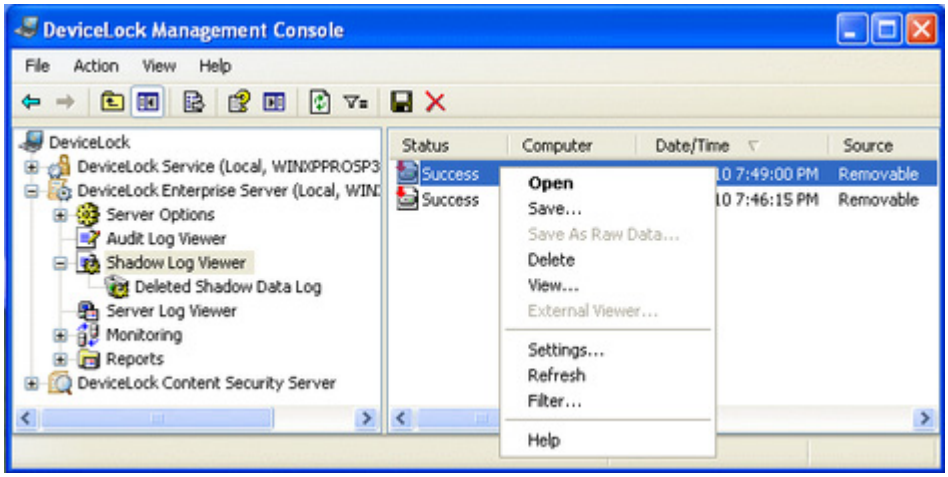
There is not much difference between the service's audit log filter and the server's audit log filter, so first read the Audit Log Filter (Service) section of this manual.

In comparison with the service's audit log filter, the server's filter has the following additional fields:

- **Computer** – this text matches a value in the Audit Log Viewer's **Computer** column. This field is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Event ID** – this number matches a value in the Audit Log Viewer's **Event** column.
  You can enter multiple values separated by a semicolon (;).
- **Received Date/Time** – specifies the time period to filter events based on when they were received by DeviceLock Enterprise Server. **From:** specifies the earliest date and time from which you want events while **To:** specifies the latest date and time from which you want events. The possible values of the **From:** parameter are: **First Event**, **Events On**. Select **First Event** to see events starting with the first event received by DeviceLock Enterprise Server. Select **Events On** to see events that were received starting with a specific date and time. The possible values of the **To:** parameter are: **Last Event**, **Events On**. Select **Last Event** to see events ending with the last event received by DeviceLock Enterprise Server. Select **Events On** to see events that were received ending with a specific date and time.

Shadow Log Viewer (Server)

The shadow log viewer allows you to retrieve the shadow log stored on DeviceLock Enterprise Server.



There is not much difference between the service's shadow log viewer and the server's shadow log viewer, so first see "Shadow Log Viewer (Service)."

In comparison with the service's shadow log viewer, the server's viewer has only two additional columns:

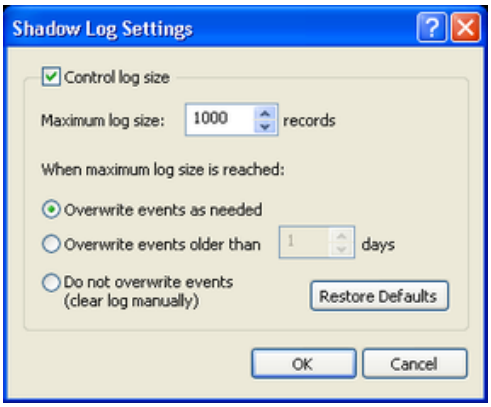
- **Computer** – the name of the computer from which shadow logs were received.
- **Received Date/Time** – the date and time when a record was received by DeviceLock Enterprise Server.

Also, unlike the service's shadow log viewer, when you delete a record in the server's viewer, the record's binary data is removed from the database or from the disk (it depends on the Store shadow files in SQL Server flag) but all other information (such as the file name and size, user name, date/time, process and so on) is moved to the special log called Deleted Shadow Data Log.

This Deleted Shadow Data Log is used when you do not need the content of the shadow data anymore and you want to clean up storage (either SQL Server or the disk), but you need to keep information about the data transfer.

Shadow Log Settings

To define a maximum log size and what DeviceLock Enterprise Server should do if the shadow log becomes full, use **Settings** from the context menu of **Shadow Log Viewer**.



For information on these settings, see "Audit Log Settings (Server)."

When DeviceLock Enterprise Server needs to remove some old records from the shadow log because of defined parameters (**Overwrite events as needed** and **Overwrite events older than**), these records are moved to the Deleted Shadow Data Log.

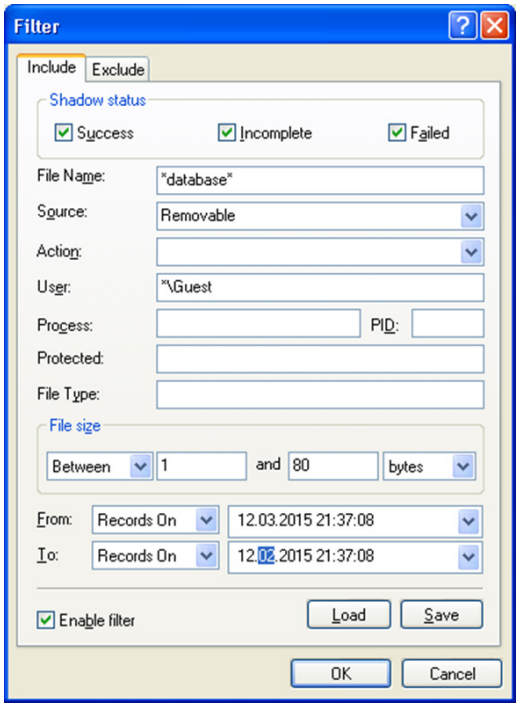
If there is no space for new records in the shadow log and there is nothing to delete then DeviceLock Enterprise Server does not remove shadowed data from remote users' computers. This prevents the loss of shadowed data due to lack of space in the log. When some space becomes available in the log, DeviceLock Enterprise Server moves the remaining shadowed data from users' computers to this log.

It is best to avoid accumulating shadowed data on users' computers. We recommend that you monitor the DeviceLock Enterprise Server's log on a periodic basis, watch for warning messages and adjust log settings appropriately.

Shadow Log Filter (Server)

You can filter data in Shadow Log Viewer so that only records that meet specified conditions are displayed in the list.

To open the **Filter** dialog box, use **Filter** from the context menu of **Shadow Log Viewer** or press the appropriate button on the toolbar.



There is not much difference between the service's shadow log filter and the server's shadow log filter, so first see "Shadow Log Filter (Service)."

In comparison with the service's shadow log filter, the server's filter has the following additional fields:

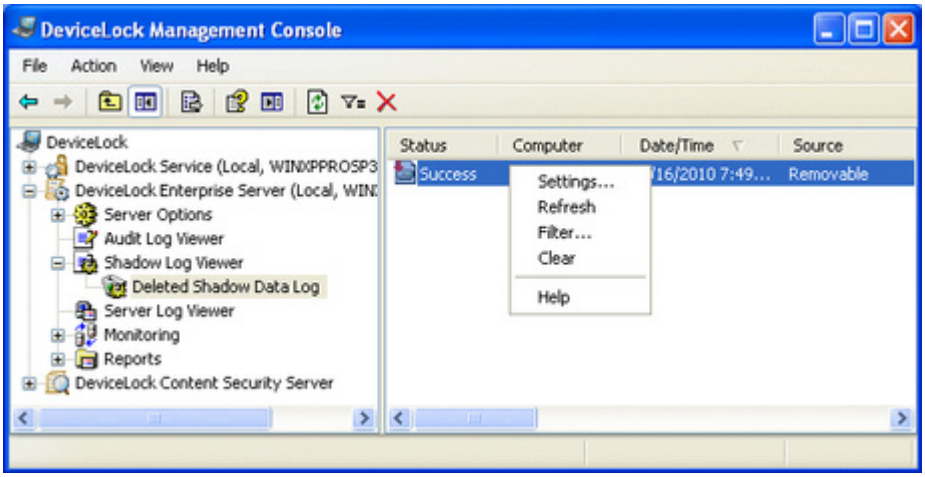
- **Computer** – the text that matches a value in the Shadow Log Viewer's **Computer** column. This field is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Received Date/Time**– specifies the time period to filter records based on when they were received by DeviceLock Enterprise Server. **From:** specifies the earliest date and time from which you want records while **To:** specifies the latest date and time from which you want records. The possible values of the **From:** parameter are: **First Record**, **Records On**. Select **First Record** to see records starting with the first record received by DeviceLock Enterprise Server. Select **Records On** to see records that were received starting with a specific date and time. The possible values of the **To:** parameter are: **Last Record**, **Records On**. Select **Last Record** to see records ending with the last record received by DeviceLock Enterprise Server. Select

Records On to see records that were received ending with a specific date and time.

Deleted Shadow Data Log

This viewer allows you to retrieve information about deleted shadow log records.

When a record is removed from the log in Shadow Log Viewer, the record's binary data is deleted but all other information (such as the file name and size, user name, date/time, process and so on) is moved to this log.



This log is used when you do not need the content of the shadow data anymore and you want to clean up the storage (either SQL Server or the disk) but at the same time you need to keep the information about the data transfer.

To define a maximum log size and instruct DeviceLock Enterprise Server regarding what it should do if the deleted shadow data log becomes full, use **Settings** from the context menu available with a right mouse click. This log's settings are similar to the audit log's settings, so see "Audit Log Settings (Server)" for more information.

If there is no space for new records in the deleted shadow data log and there is nothing to remove, then DeviceLock Enterprise Server just drops any new records. To avoid loosing records in this way, we recommend that you monitor DeviceLock Enterprise Server's log on a periodic basis and watch for warning messages there.

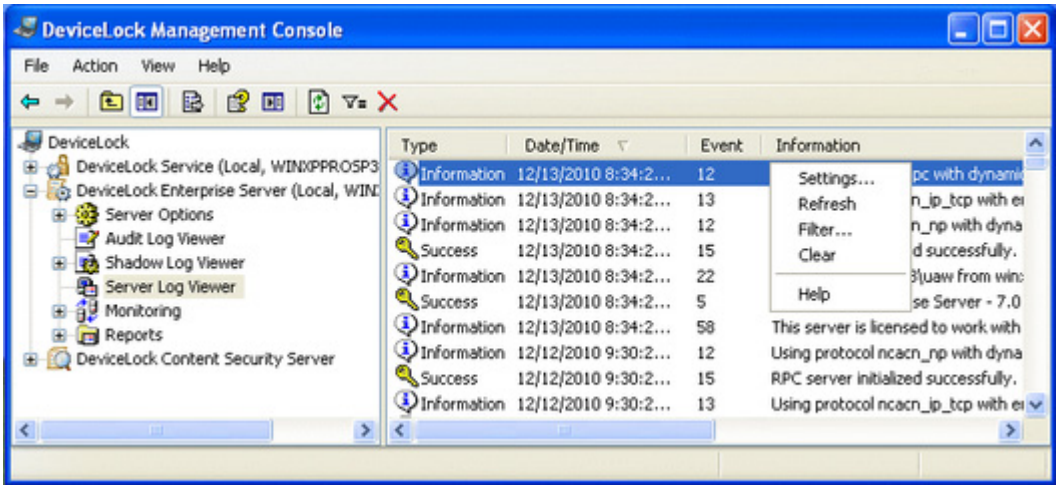
To refresh the list, select **Refresh** from the context menu available with a right mouse click or by pressing the appropriate button on the toolbar.

To filter records in this list, select **Filter** from the context menu available with a right mouse click or by pressing the appropriate button on the toolbar. The same filter is used by the Shadow Log Viewer, so see "Shadow Log Filter (Server)" for more information.

To clear all records from this log, select **Clear** from the context menu or press the appropriate button on the toolbar.

Server Log Viewer

This viewer allows you to retrieve the internal DeviceLock Enterprise Server's log. The server uses this log to write errors, warnings and other important information (such as configuration changes, start/stop events, version, and so on).



You may use the information from this log to diagnose problems (if any), to monitor changes in the server's configuration and to see who has cleared logs and when.

The columns of this viewer are defined as follows:

- **Type** – the class of an event: **Success**, **Information**, **Warning** or **Error**.
- **Date/Time** – the date and the time when an event has occurred.
- **Event** – a number identifying the particular event type.
- **Information** – event-specific information, such as error/warning descriptions, names and values of changed parameters, and so on.
- **Server** – the name of the server where an event occurred.
- **Record N** – the record number.

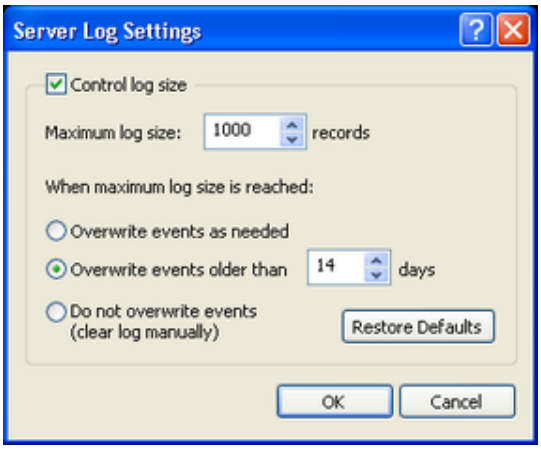
To refresh the list, select **Refresh** from the context menu available by clicking the right mouse button or by pressing the appropriate button on the toolbar.

To clear all records from this log, select **Clear** from the context menu or press the appropriate button on the toolbar.

After the server's log is cleared, the one event about this clearing action is written into the log (for example, "The Server Log (100 record(s)) was cleared by VM2000AD\Administrator from xpvirt.vm2000ad.com").

Server Log Settings

To define a maximum log size and what DeviceLock Enterprise Server should do if the server's log becomes full, use **Settings** from the context menu of **Server Log Viewer**.

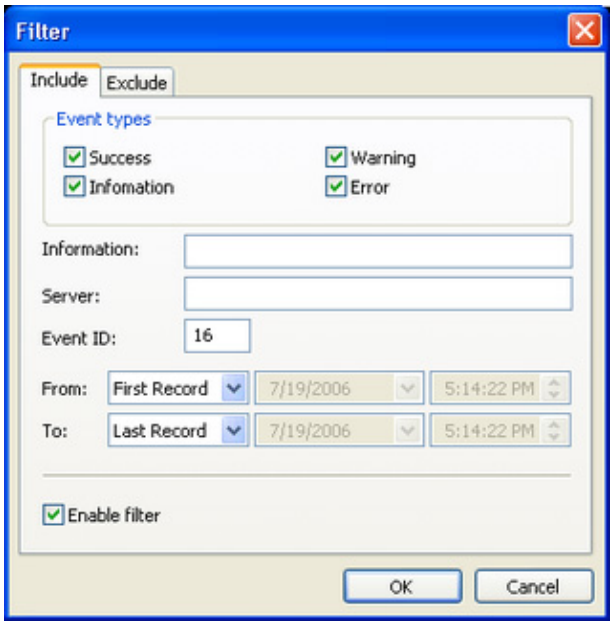


For information on these settings, see "Audit Log Settings (Server)."

If there is no space for new records in the server's log and there is nothing to remove, then DeviceLock Enterprise Server just drops any new records.

Server Log Filter

You can filter data in the Server Log Viewer so that only records that meet specified conditions are displayed in the list. To open the **Filter** dialog box, use **Filter** from the context menu of **Server Log Viewer** or press the appropriate button on the toolbar.



There are no big differences between defining an Audit Log Filter and a Server Log Filter, so for more information, see "Audit Log Filter (Service)."

When the filter is active you can define its condition by entering values into the following fields:

- **Success** – specifies whether to filter events of the **Success** class.
- **Information** – specifies whether to filter events of the **Information** class.
- **Warning** – specifies whether to filter events of the **Warning** class.
- **Error** – specifies whether to filter events of the **Error** class.
- **Information** – the text that matches a value in the Server Log Viewer's **Information** column. This field is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Server** – the text that matches a value in the Server Log Viewer's **Server** column. This field is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Event ID** – the number that matches a value in the Server Log Viewer's **Event** column.
  You can enter multiple values separated by a semicolon (;).
- **From** – specifies the beginning of the interval of events that you want to filter. Select **First Event** to see events starting with the first event recorded in the log. Select **Events On** to see events that occurred starting with a specific time and date.
- **To** – specifies the end of the range of events that you want to filter. Select **Last Event** to see events ending with the last event recorded in the log. Select **Events On** to see events that occurred ending with a specific time and date.

Monitoring

This functionality of DeviceLock Enterprise Server allows you to implement real-time monitoring of DeviceLock Services across the network. DeviceLock Enterprise Server can monitor remote computers in real-time, checking DeviceLock Service status (running or not), policy consistency and integrity. The detailed information is written to the special log and can be viewed using the Monitoring Log Viewer.

Also, it is possible to define a master policy that can be automatically applied across selected remote computers in the event that their current policies are suspected to be out-of-date or damaged.

With the DeviceLock Enterprise Server's Monitoring functionality, it is now possible to distribute DeviceLock Service agents to client computers, which allows for an additional way to deploy DeviceLock Service beyond the traditional methods (software installation GPO,

Microsoft SCCM, DeviceLock consoles, local Setup.exe, etc.). For more information, see "Installation via DeviceLock Enterprise Server".

Moreover, you can use this policy recovery feature as an alternative way of deploying settings, permissions, audit, shadowing rules and alerts to remote DeviceLock Services across the network.

Architecture Overview

All actions (computers monitoring, policy consistency and integrity checking, etc.) are performed by tasks.

On a single DeviceLock Enterprise Server, you can have as many tasks as you wish. The maximum number of tasks on one server is only limited by available memory, CPU and network's bandwidth capacity. Please keep in mind that the server should have enough resources to communicate with at least 10 remote computers simultaneously.

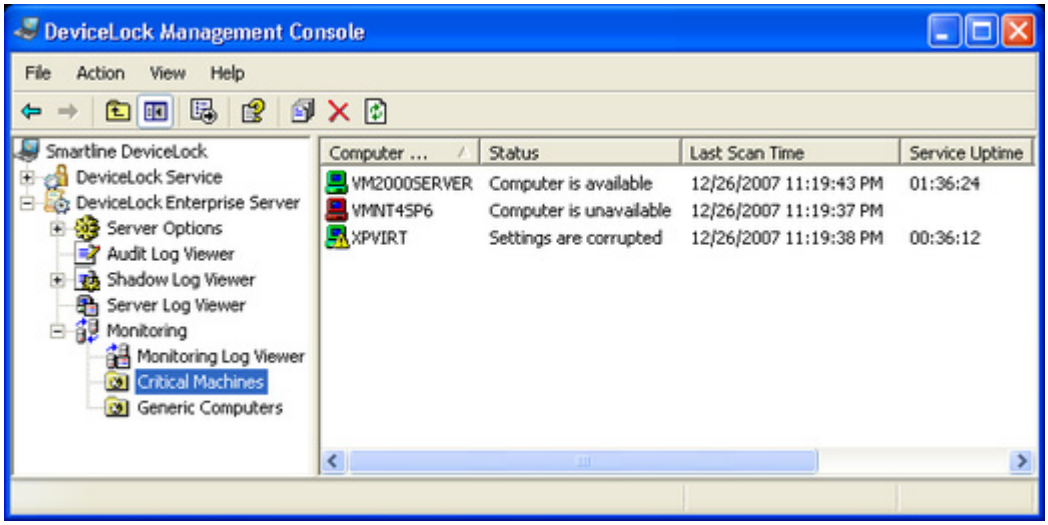
By default, DeviceLock Enterprise Server can execute up to 30 tasks simultaneously. This means that if you have, for example, 40 tasks and all of them run at the same time, the first 30 tasks will run first and each of the remaining 10 tasks will run as soon as others complete.

However, you can change the number of tasks that can be run simultaneously by modifying the registry. To define the new number, open **Regedit** and set the following entry on the computer where DeviceLock Enterprise Server is running:

- Key: **HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockEnterpriseServer**
- Name: **ConcurrentJobs**
- Type: **DWORD**
- Value: *number_of_threads*
  where *number_of_threads* must be a value between 1 and 1000.

During their execution, tasks write status information to the monitoring log including data about monitored computers and DeviceLock Services. They'll also write possible errors which occurred during the scanning of computers and connecting to DeviceLock Services.

Also, tasks display the status of monitored computers and other useful information at the management console. This allows you to keep an eye on monitored computers in real-time.



To view the monitored computers that belong to the task, select this task in the console tree.

To refresh the information displayed in the computers list, select **Refresh** from the context menu available by a right mouse click or press the appropriate button on the toolbar.

- **Computer Name** – the name of the monitored computer.
- **Status** – the status of the monitored computer and DeviceLock Service.

  The status also affects the small picture (an icon) displayed next to the **Computer Name** parameter. The general rules for interpreting computer icons are:

  - Green computer – means that the computer is working and DeviceLock Service is running on it.
  - Red computer – means that the computer is not working/not found, or it is working but without DeviceLock Service.
  - Computer with exclamation mark – means that something is wrong with the computer or DeviceLock Service.

  There can be eight different statuses:

  1. **Computer is available** – this status means that the monitored computer is working and DeviceLock Service is running on it. Also, if this task verifies policy integrity, then verification happened without any errors. The computer's icon will be "green computer".

     If this task restores the broken policy, the computer's icon will be "green computer with exclamation mark".
  2. **Computer is unavailable** – this status means that DeviceLock Enterprise Server is unable to scan the monitored computer. This occurs when a computer is not working or connections are blocked by a firewall, but the computer's name/address can be resolved through DNS. The computer's icon will be "red computer".
  3. **Service is unavailable** – this status means that DeviceLock Enterprise Server is unable to connect to DeviceLock Service on the monitored computer. This occurs when the computer is working but DeviceLock Service

is not running. Also, it could be the result of running DeviceLock Service on a different TCP port than that specified in the task configuration or due to connections being blocked by the firewall. The computer's icon will be "red computer with exclamation mark". For more information on connection issues, see the description of the Service connection settings parameter.

4. **Settings are corrupted** – this status means that the monitored computer is working and DeviceLock Service is running on it but the policy verification process has failed. This happens when the master policy is assigned to a task and it differs from the monitored DeviceLock Service policy. The computer's icon will be "green computer with exclamation mark".
5. **Unresolved computer address** – this status means that DeviceLock Enterprise Server is unable to resolve the name/address of the computer. This happens when an invalid computer name that does not exist in DNS is specified. Also, it could happen because there is no DNS server. In this case the **Unresolved computer address** status should be treated as **Computer is unavailable**. The computer's icon will be "red computer with exclamation mark".
6. **Unsupported service version** – this status means that DeviceLock Enterprise Server is trying to download a policy (service settings) from DeviceLock Service version 6.2 and lower. The policy verification is supported only for version 6.2.1 and later. The computer's icon will be "green computer with exclamation mark".
7. **Access is denied** – this status means that DeviceLock Enterprise Server is unable to connect to DeviceLock Service due to lack of privileges. It happens when the account under which the DeviceLock Enterprise Server service starts has no rights to connect to DeviceLock Service. The computer's icon will be "green computer with exclamation mark". For more information on how to resolve this issue, see the description of the Service connection settings parameter.
8. **No License** – this status means that DeviceLock Enterprise Server is unable to monitor the computer running DeviceLock Service due to an insufficient number of licenses. DeviceLock Enterprise Server handles as many DeviceLock Service instances as there are licenses loaded into DeviceLock Enterprise Server. For more information, see "License information" in "Installing DeviceLock Enterprise Server". The computer's icon will be "green computer with exclamation mark".

Also, the same status messages (except **Computer is available**) are written to the monitoring log so you can overview the situation with monitored computers later.

- **Last Scan Time** – the date and time of the last scan attempt. This scan attempt can be either successful or not.
- **Last Successful Scan Time** - the date and time of the last successful scan attempt.
- **Service Uptime** – shows how long DeviceLock Service has been working on the monitored computer.
- **Computer Uptime** – shows how long the monitored computer has been working. By comparing the computer's uptime with the service's uptime (see above) you can

always see whether or not DeviceLock Service was stopped during the current computer's session.

- **Service Version** – the version of DeviceLock Service. Last five digits indicate the build number.

Monitoring Algorithm

The algorithm used in the monitoring process is simple but effective:

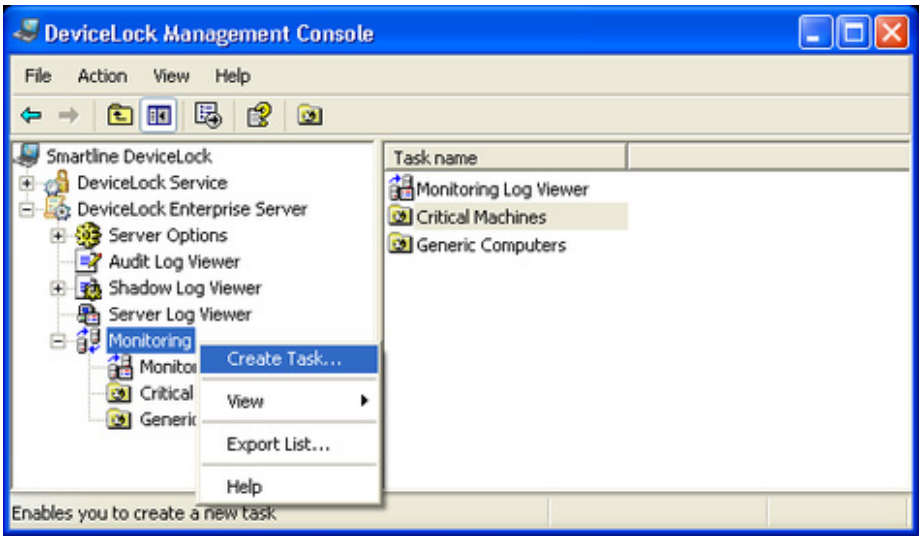
1. First of all DeviceLock Enterprise Server tries to scan the monitored computer to determine whether or not it is working. If the scan succeeds then the computer receives the **available** status and computer monitoring continues. Otherwise, it receives the **unavailable** status and computer monitoring stops (the record is written to the monitoring log).
2. Then DeviceLock Enterprise Server tries to connect to DeviceLock Service. If the connection succeeds then DeviceLock Service receives the **available** status and computer monitoring continues. Otherwise, it receives the **unavailable** status and computer monitoring stops (the record is written to the monitoring log).
3. If this task should verify DeviceLock Service policy integrity then computer monitoring continues. Otherwise, computer monitoring stops (nothing logged).
4. DeviceLock Enterprise Server downloads the policy from DeviceLock Service and compares it with the master policy assigned to this task. If no difference is found computer monitoring stops (nothing logged). If there is a difference between the two policies then computer monitoring continues (the record is written to the monitoring log).
5. If this task should restore the broken policy, then DeviceLock Enterprise Server writes the master policy to DeviceLock Service and computer monitoring stops (the record is written to the monitoring log). Otherwise, computer monitoring just stops (nothing logged).

If some error occurs at any step described above, then the record about that will be written to the monitoring log. If this error is not critical, computer monitoring may continue. If it is a critical error then computer monitoring stops.

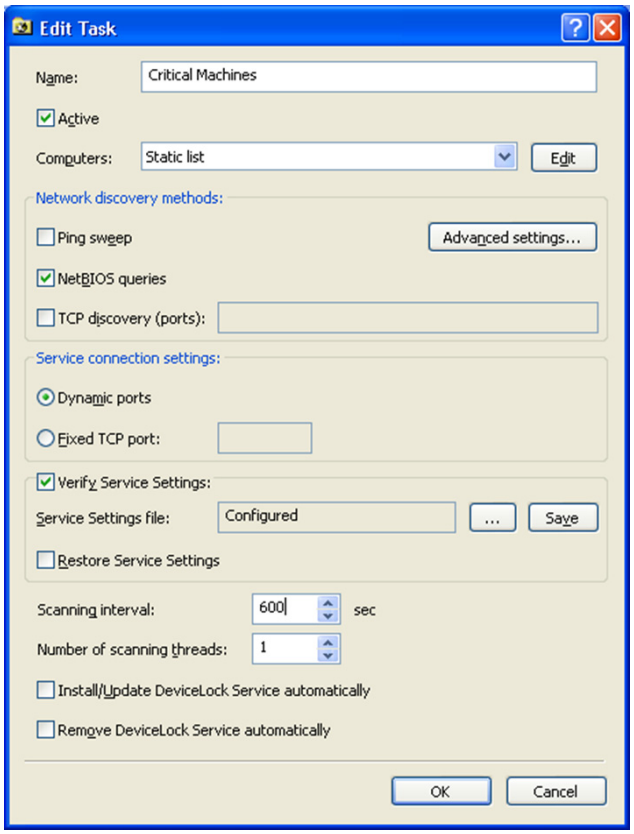
Also, some very critical errors (such as "no memory") can halt execution of the whole task.

Create / Modify Task

Each task contains its own set of computers, actions and configuration parameters.



To create a new task, use **Create Task** from the context menu of the **Monitoring** item. To edit an existing task, select this task in the console tree and use **Edit Task** from the context menu. If you wish to delete the task permanently, select this task in the console tree and use **Delete Task** from the context menu.



Name – the name of the task used to identify this task in the tasks list and in the monitoring log.

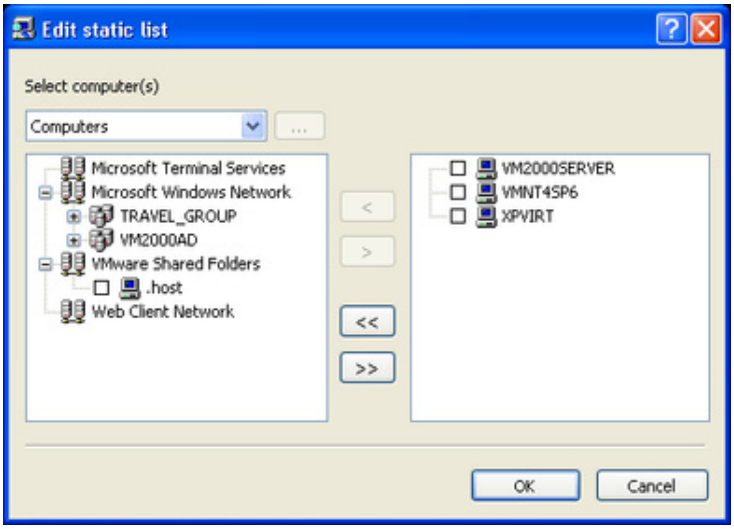
Active – if selected, allows DeviceLock Enterprise Server to execute this task. Clear this check box if you wish to disable the task but do not want to delete it permanently.

Computers – the type of the computers list used to define what computers will be monitored by this task.

Click the **Edit** button to configure the list selected in **Computers**.

Two computer list types are supported:

1. **Static list** – all of the computers are specified in the list by their names or IP addresses. Since this list is static, even if some computer no longer exists in the network, it will be monitored (and the error logged) until its record is deleted from the list manually.



Computers that will be monitored should be specified in the right list. You have to select needed computers in the left list and then move them to the right list by clicking the **>** button.

If you need to exclude some computers from the monitoring process, select them in the right list and then click the **<** button.

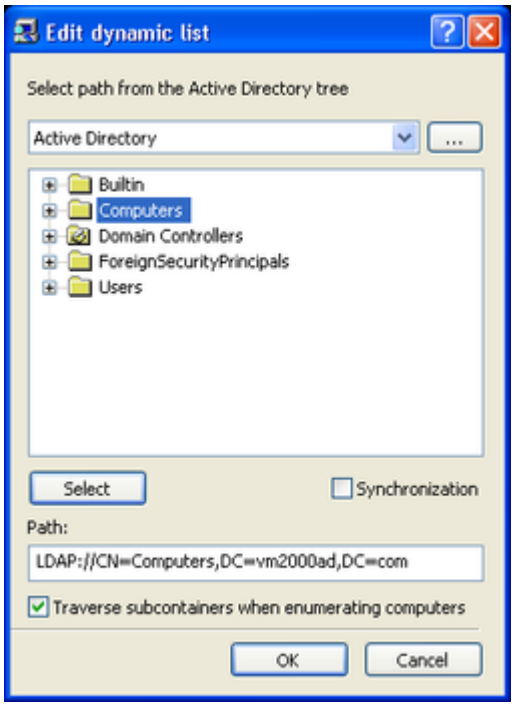
By using **>>** and **<<** buttons, you can add and remove all available computers at the same time (no need to select computers in the list).

There are several flexible ways to choose network computers from the left list:

- **Active Directory** – you browse Active Directory organizational units (OUs) and select computers.
- **Computers** – you browse the network tree and select computers.

- **LDAP** – you browse the LDAP (Lightweight Directory Access Protocol) tree and select computers from the directory.
- **From File** – you load a predefined list of computers from the external text file and then select the computers. To open an external file, click the **...** button. A text file must contain each computer's name or IP address on separate lines and can be either Unicode or non-Unicode.
- **Manual** – you type computer names manually to select the computers. Each computer's name or IP address must be typed on a separate line.

2. **Dynamic list** – instead of computer names or IP addresses, the dynamic list contains a path to the container (for example, an organizational unit) in the directory service tree (such as Active Directory, Novell eDirectory, OpenLDAP and so on). Each time the task is executing, DeviceLock Enterprise Server retrieves all the computers that currently exist in this container. Hence, if some computer was removed from the directory tree or moved to another container it will not be monitored anymore. And vice versa, if there is some new computer that did not exist in the container at the time the task was created/modified, but was added to this container later, it will be retrieved and monitored at the time of executing the task.



A path to the container from which computers will be retrieved at the time of executing the task, should be specified in the **Path** parameter. You must use the LDAP string representation for distinguished names.

You may browse the directory tree and choose the needed container by clicking the **Select** button. In this case a path to this container will be specified in the **Path** parameter automatically.

Select the **Traverse subcontainers when enumerating computers** check box to allow DeviceLock Enterprise Server to retrieve computers from all the nested containers located inside the selected container. Otherwise, if this check box is unselected all nested containers are ignored, and only computers located directly in the selected container are retrieved at the time of executing the task.

There are two modes to work with the directory service:

- **Active Directory** – You browse the Active Directory tree and select the needed container.

  While the Active Directory tree can also be displayed by choosing the **LDAP** option (see below), the Active Directory mode results in greater efficiency between the directory service and DeviceLock Enterprise Server service and thus resource savings.

  If you need to supply alternative credentials to access Active Directory, click the **...** button to open the **Credentials** dialog box and specify the needed user account and its corresponding password.

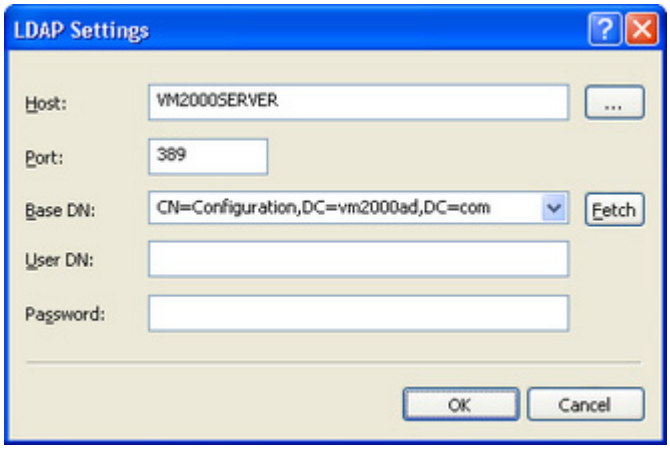
Note: If no alternative credentials are specified when accessing Active Directory, DeviceLock Enterprise Server uses the credentials of the account under which its service started. For more information, see the description of the Log on as parameter.

Select the **Synchonization** check box to allow DeviceLock Enterprise Server to use the internal synchronization mechanisms provided by Active Directory. This will dramatically reduce the load on the domain controller and speed up the process of retrieving computers at the time of task execution.

Note: Administrative access to Active Directory is required to use the synchronization function.

- **LDAP** – You browse the LDAP (Lightweight Directory Access Protocol) tree and select the needed container.

  To configure a connection to the LDAP server, click the **...** button and open the **LDAP Settings** dialog box.



Host – the name or the IP address of the LDAP server to connect to.

Port – the TCP port on which the LDAP server accepts connections. The default port is 389.

Base DN – the starting point for you to browse the directory tree. You must use the LDAP string representation for distinguished names (for example, cn=qa,o=SMARTLINE,c=US). Leave the **Base DN** box blank to start browsing from the root.

By clicking the **Fetch** button, you can get all the published naming contexts.

User DN – the distinguished name (DN) of the directory user that allows connection to the directory. You must use the LDAP string representation for distinguished names (for example, cn=admin,o=SMARTLINE,c=US).

Note: If no user is specified when accessing the LDAP server, DeviceLock Enterprise Server uses the credentials of the account under which its service started. For more information, see the description of the Log on as parameter.

Password – the user's password.

Network discovery methods – types of network scanning that will be used to determine the status (**available** or **unavailable**) of monitored computers.

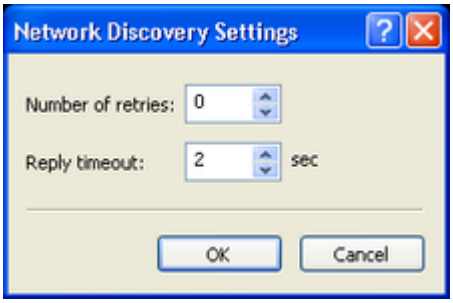
Upon executing the task, DeviceLock Enterprise Server uses all selected discovery methods in their given order until the status **available** is returned for the target computer. If none of the selected methods returns the **available** status, then the target computer receives the **unavailable** status.

Three types of the network scan are supported:

1. **Ping sweep** – DeviceLock Enterprise Server sends a regular ICMP ping to the target computer and then waits for its reply.
2. **NetBIOS queries** – if the Client for Microsoft Networks is installed on the target computer, then this computer will answer the NetBIOS type query sent by DeviceLock Enterprise Server.
3. **TCP discovery (ports)** – DeviceLock Enterprise Server checks for a particular open TCP port on the target computer. Using the comma (,) or semicolon (;) as a separator, you can specify several ports so they will be checked one by one in their given order.

Note: A firewall running on a target computer can block the sending of some or all network packets so such a computer will be detected as unavailable even if it is switched on and working.

To define additional parameters for discovery methods, click the **Advanced settings** button and open the **Network Discovery Settings** dialog box.



- **Number of retries** – the number of times that DeviceLock Enterprise Server will perform each type of scan when it returns the **unavailable** status. 0 means that no retries will be performed for that scan type after the first failed attempt.
- **Reply timeout** – the time in seconds DeviceLock Enterprise Server will actually wait for a response from the target computer for each type of scan. If DeviceLock Enterprise Server is running on a slow or busy network you may need to increase this timeout.

Service connection settings – these options define how DeviceLock Enterprise Server should connect to DeviceLock Services on the monitored computers to obtain service version, settings, etc. If the correct connection settings are not specified, DeviceLock Enterprise Server will not be able to connect to monitored services and their computers will not receive the **available** status.

DeviceLock Service can be configured to use either a fixed port or dynamic ports during the installation process. For more information on this, see "Unattended Installation" and "Remote Installation via DeviceLock Enterprise Manager."

There are two connection options:

- **Dynamic ports** – to instruct DeviceLock Enterprise Server to use dynamic ports for communication with DeviceLock Service, select this option.
- **Fixed TCP port** – if DeviceLock Service is configured to accept connections on a fixed port, then you should select this option and specify that port number.

Note: In order to successfully connect to monitored DeviceLock Services and obtain needed information from them, DeviceLock Enterprise Server must have at least Read-only access rights to these services. If this task also needs to write some settings to monitored DeviceLock Services, then DeviceLock Enterprise Server requires Full access rights to these services.

To connect to monitored DeviceLock Services, DeviceLock Enterprise Server uses the credentials of the account under which its service started. It can also use DeviceLock Certificate authentication, if a private key is specified. For more information, see the description of parameters Log on as and Certificate Name.

Verify Service Settings – select this check box if you want to verify policy integrity for DeviceLock Services running on monitored computers.

- **Service Settings file** – to assign the master policy to the task, you should load the XML file with service settings (the master policy file). This master policy file can be created using DeviceLock Management Console, DeviceLock Group Policy Manager and/or DeviceLock Service Settings Editor.

  During the policy verification process, DeviceLock Enterprise Server downloads the policy from each monitored DeviceLock Service and compares it with the master policy assigned to this task.

  All unconfigured parameters (those which have the **Not Configured** state) in the master policy are ignored during the policy verification process. Using this feature you can monitor the integrity of only the most important parameters and allow other parameters to be changed without being reported to the monitoring log.

  To load the master policy file, click the **...** button. Since the signature is not validated at this step, it can be either a signed or non-signed file. However, if you load the signed file then its name will be displayed in the **Service Settings file** box in round brackets.

If you are modifying the task and the master policy is already assigned, you can export it to an external XML file by clicking the **Save** button.

- **Restore Service Settings** – if selected, DeviceLock Enterprise Server will overwrite the current policy of a monitored DeviceLock Service for which the policy verification process failed with the master policy assigned to this task. Using this feature you can not only passively monitor the integrity of specific parameters but also restore them in case they were changed.

Scanning interval – the time in seconds that should pass after a task completes and before DeviceLock Enterprise Server will start executing the same task again.

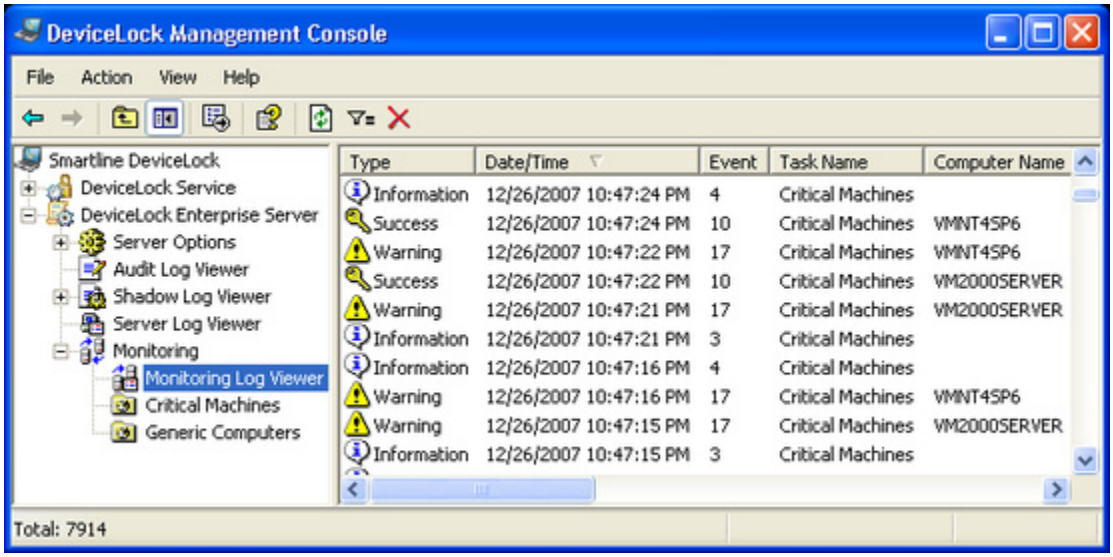
Number of scanning threads – the maximum number of threads that can be used by this task simultaneously. You can increase this number to parallelize the process of computer scanning. However, a larger number of threads requires more hardware resources (especially RAM and network bandwidth) for DeviceLock Enterprise Server.

Install/Update DeviceLock Service automatically – select this checkbox if you want to install DeviceLock Service to monitored computers.

Remove DeviceLock Service automatically – select this checkbox if you want to remove DeviceLock Service from monitored computers.

Monitoring Log Viewer

This viewer allows you to retrieve the monitoring log. The monitoring log is used by tasks to write information about monitored computers and DeviceLock Services.


DeviceLock Management Console
File Action View Help
Smartline DeviceLock
DeviceLock Service
DeviceLock Enterprise Server
Server Options
Audit Log Viewer
Shadow Log Viewer
Server Log Viewer
Monitoring
Monitoring Log Viewer
Critical Machines
Generic Computers
Type Date/Time Event Task Name Computer Name
Information 12/26/2007 10:47:24 PM 4 Critical Machines
Success 12/26/2007 10:47:24 PM 10 Critical Machines VMNT4SP6
Warning 12/26/2007 10:47:22 PM 17 Critical Machines VMNT4SP6
Success 12/26/2007 10:47:22 PM 10 Critical Machines VM2000SERVER
Warning 12/26/2007 10:47:21 PM 17 Critical Machines VM2000SERVER
Information 12/26/2007 10:47:21 PM 3 Critical Machines
Information 12/26/2007 10:47:16 PM 4 Critical Machines
Warning 12/26/2007 10:47:16 PM 17 Critical Machines VMNT4SP6
Warning 12/26/2007 10:47:15 PM 17 Critical Machines VM2000SERVER
Information 12/26/2007 10:47:15 PM 3 Critical Machines
Total: 7914

The columns of this viewer are defined as follows:

- **Type** – the class of an event: **Success**, **Information**, **Warning** or **Error**.

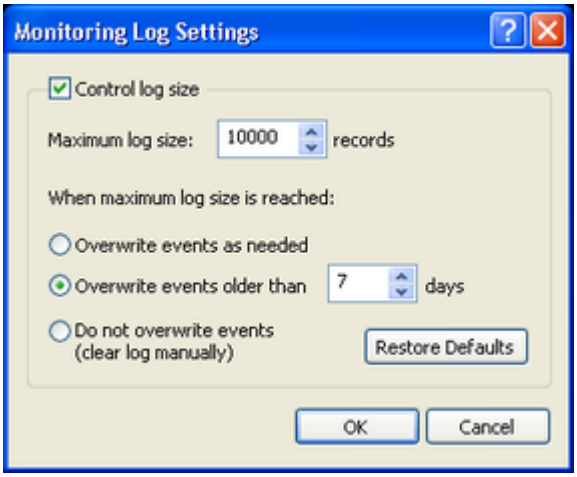
- **Date/Time** – the date and the time when an event has occurred.
- **Event** – a number identifying the particular event type.
- **Task Name** – the name of the task responsible for this event. Can be empty if an event does not link to any task.
- **Computer Name** – the name of the computer belonging to the task that is responsible for this event. Can be empty if an event does not link to the computer.
- **Information** – event-specific information, such as status, error, warning, and so on.
- **Server** – the name of the server where an event occurred.
- **Record N** – the record number.

To refresh the list, use **Refresh** from the context menu available by clicking the right mouse button or by pressing the appropriate button on the toolbar.

To clear all records from this log, use **Clear** from the context menu or press the appropriate button on the toolbar.

Monitoring Log Settings

To define a maximum log size and instruct DeviceLock Enterprise Server in the event the monitoring log becomes full, use **Settings** from the context menu of the **Monitoring Log Viewer**.

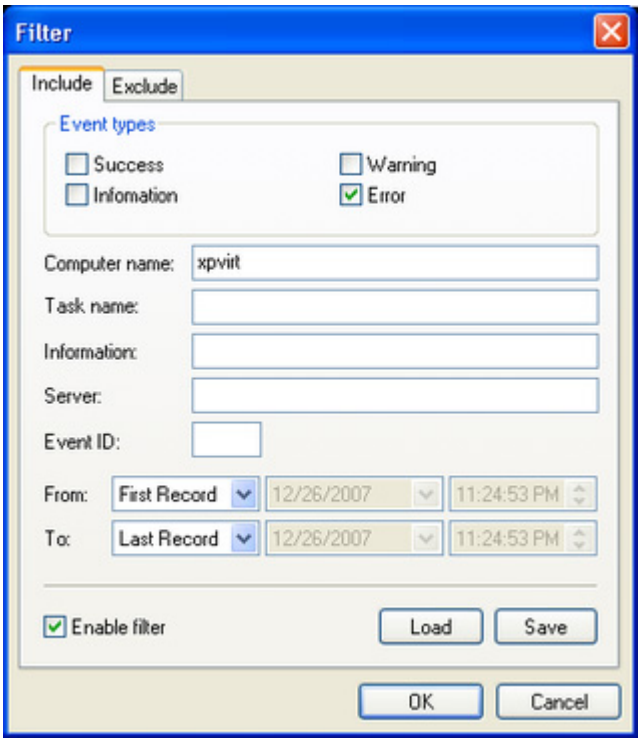


For information on these settings, see Audit Log Settings (Server).

Monitoring Log Filter

You can filter data in the Monitoring Log Viewer so that only records that meet specified conditions are displayed in the list.

To open the **Filter** dialog box, use **Filter** from the context menu of the **Monitoring Log Viewer** or press the appropriate button on the toolbar.



There is no significant difference between defining an Audit Log Filter and a Monitoring Log Filter, so for more information see "Audit Log Filter (Service)."

When the filter is active you can define its condition by entering values into the following fields:

- **Success** – specifies whether to filter events of the **Success** class.
- **Information** – specifies whether to filter events of the **Information** class.
- **Warning** – specifies whether to filter events of the **Warning** class.
- **Error** – specifies whether to filter events of the **Error** class.
- **Computer Name** – the text that matches a value in the Monitoring Log Viewer's **Computer Name** column. This field is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Task Name** – the text that matches a value in the Monitoring Log Viewer's **Task Name** column. This field is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Information** – the text that matches a value in the Monitoring Log Viewer's **Information** column. This field is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).

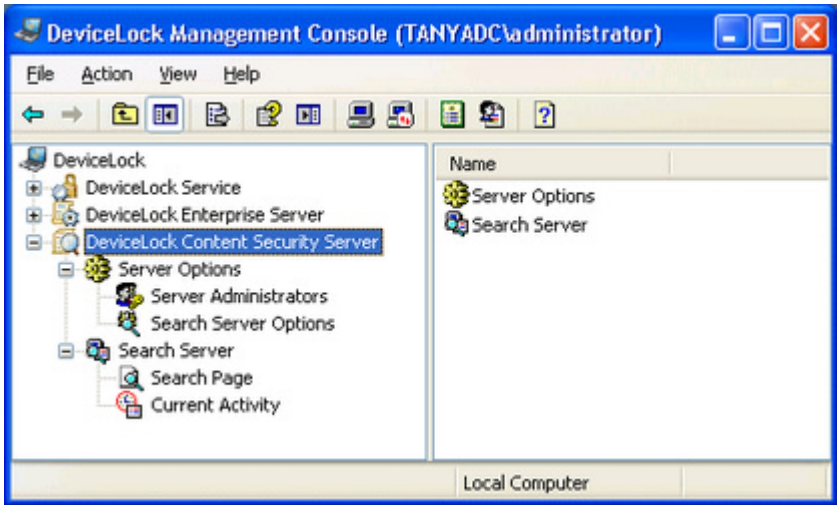
- **Server** – the text that matches a value in the Monitoring Log Viewer's **Server** column. This field is not case-sensitive and you may use wildcards.
  You can enter multiple values separated by a semicolon (;).
- **Event ID** – the number that matches a value in the Monitoring Log Viewer's **Event** column.
  You can enter multiple values separated by a semicolon (;).
- **From** – specifies the beginning of the interval of events that you want to filter. Select **First Event** to see events starting with the first event recorded in the log. Select **Events On** to see events that occurred starting with a specific time and date.
- **To** – specifies the end of the range of events that you want to filter. Select **Last Event** to see events ending with the last event recorded in the log. Select **Events On** to see events that occurred ending with a specific time and date.

Managing and Using DeviceLock Content Security Server

Navigating DeviceLock Content Security Server

Before addressing the functionality of DeviceLock Content Security Server, you need to examine how to perform basic navigation.

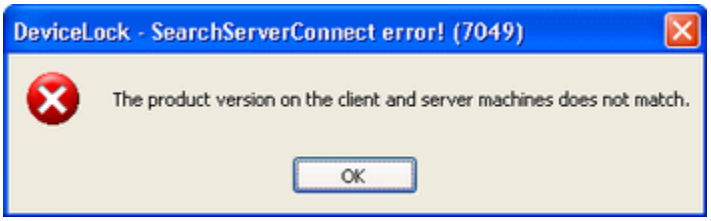
Use the **DeviceLock Content Security Server** node in DeviceLock Management Console to configure and use DeviceLock Content Security Server.



Right-click the **DeviceLock Content Security Server** node to display the following commands:

- **Connect** – connects to the computer running DeviceLock Content Security Server. For more information, see "Connecting to Computers."

  When you connect to a computer where an old version of DeviceLock Content Security Server is installed, you may receive the following message:

  In this case you need to install the new version of DeviceLock Content Security Server on this computer. For information on how to install DeviceLock Content Security Server, see "Installing DeviceLock Content Security Server."
- **Reconnect** – connects to the currently connected computer once again.
- **Connect to Last Used Server at Startup** – click this command to instruct DeviceLock Management Console to automatically connect to the last used server each time the console starts up.
- **Certificate Generation Tool** – runs the special tool that allows you to generate DeviceLock Certificates. For more information, see "Generating DeviceLock Certificates."
- **DeviceLock Signing Tool** – runs the special tool that allows you to grant users temporary access to requested devices and sign XML files with DeviceLock Service settings. For more information, see "DeviceLock Signing Tool."
- **About DeviceLock** – displays the dialog box with information about the DeviceLock version and your licenses.

Expand the **DeviceLock Content Security Server** node to display the following sub-nodes:

- The **Server Options** node. Use this node to configure DeviceLock Content Security Server and Search Server.

  The following list describes the general settings that you can configure for DeviceLock Content Security Sever:

  - **Server Administrators** – Use this setting to specify members of the Server Administrators group and their associated access rights.
  - **DeviceLock certificate** - Use this setting to install or remove DeviceLock Certificate.
  - **Service startup account** - Use this setting to specify the startup account information, such as the account name and the password, for the server service.
  - **TCP port** - Use this setting to specify the TCP port that the server uses to connect to DeviceLock Management Console.

  The following list describes the full-text search related settings that you can configure for Search Server:

- **DeviceLock Enterprise Server(s)** - Use this setting to specify DeviceLock Enterprise Server(s) whose data will be indexed for full-text search.
- **Index directory** - Use this setting to specify the location of the full-text index.
- **Indexing interval** - Use this setting to specify the time interval, in minutes, between the end of one indexing process and the start of the next indexing process.
- **Merge Interval**- Use this setting to specify the time interval, in minutes, at which to perform merge operations.
- **Extract text from binary** - Use this setting to allow or disallow the index to include textual information from binary data.
- **Extract text from images (OCR)** – use this setting to allow or disallow the index to include textual information from images. You can select up to 8 languages in the setting's dialog box.
- **Search Server License(s)** - Use this setting to install the required number of Search Server licenses.

- The **Search Server** node. Use this node to perform a search operation and monitor the current indexing activity.

Configuring General Settings for DeviceLock Content Security Server

There are two types of configuration settings for DeviceLock Content Security Server:

- **General settings for DeviceLock Content Security Server.** These settings affect your whole DeviceLock Content Security Server deployment.
- **Full-text search settings for Search Server.** These settings are related to full-text search and affect only the Search Server component of DeviceLock Content Security Server. For more information, see "Configuring Full-Text Search Settings for Search Server."

You can configure general server settings during the initial installation of DeviceLock Content Security Server, or you can use DeviceLock Management Console to configure and/or modify them after the server has been installed and is functioning.

Note: You must be a member of the Server Administrators group and have sufficient rights to manage and use DeviceLock Content Security Server.

Before you can use DeviceLock Management Console, you must connect it to the computer on which DeviceLock Content Security Server is installed and running. To do so, in the console tree, right-click **DeviceLock Content Security Server**, and then click **Connect**. For more information, see "Connecting to Computers."

With DeviceLock Management Console, you can perform the following configuration tasks:

- Configure which users have access to DeviceLock Content Security Server.
- Change the startup account information, such as the account name or the password, for the DeviceLock Content Security Server service.
- Install or remove DeviceLock Certificate used to authenticate communications between DeviceLock Content Security Server and DeviceLock Enterprise Server.

- Change the TCP port that DeviceLock Content Security Server uses to connect to DeviceLock Management Console.

You can perform these tasks individually or collectively.

To perform the tasks collectively, you can use the DeviceLock Content Security Server wizard. This is the wizard that starts automatically when you install or upgrade DeviceLock Content Security Server.

To perform configuration tasks collectively

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, right-click **Server Options**, and then click **Properties**.

   The first page of the wizard appears.

3. Move through the wizard. After completing each page, move to the following one by clicking **Next**, or move to the preceding one by clicking **Back**. On the final page, click **Finish** to complete the wizard.

   For detailed information on how to configure DeviceLock Content Security Server using the configuration wizard, see "Installing DeviceLock Content Security Server."

Below are step-by-step instructions explaining how to perform individual configuration tasks using DeviceLock Management Console.

Task: Configure which users have access to DeviceLock Content Security Server

You can select users you want to have access to your DeviceLock Content Security Server. This restricts outsiders from accessing or damaging the server.

To configure which users have access to the server

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, do one of the following:
   - Select **Server Options**. In the details pane, double-click **Server Administrators** or right-click **Server Administrators** and then click **Properties**.
     When you select Server Options in the console tree, they are displayed in the details pane.

     - OR –
   - Expand **Server Options**. Under **Server Options**, right-click **Server Administrators** and then click **Properties**.

   The DeviceLock Content Security Server dialog box appears.

3. In the **DeviceLock Content Security Server** dialog box, do the following:

TO DO THIS	FOLLOW THESE STEPS
To enable default	• Select the **Enable Default Security** check box. *If default security is enabled, members of the local*

TO DO THIS	FOLLOW THESE STEPS
security	*Administrators group will have full access to DeviceLock Content Security Server*.
To restrict access to the server to specific users	1. Clear the **Enable Default Security** check box. 2. Under **Users**, click **Add** to add the specific users to whom you want to allow access to DeviceLock Content Security Server. *The Select Users or Groups dialog box appears*. 3. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**. *The users and groups you selected are added to the Server Administrators group and are displayed under Users in the DeviceLock Content Security Server dialog box*. *Server Administrators are users or groups that are authorized to perform tasks related to configuring and using DeviceLock Content Security Server. By default, members of the Server Administrator group have full access rights to the server.* To change their access rights, under **Users**, select the user or group and then click any option in the access rights list. The available options are: • **Full Access** – enables full access to DeviceLock Content Security Server. Users can install/uninstall DeviceLock Content Security Server, connect to it using DeviceLock Management Console, change its settings and run search queries. • **Change** - enables change access to DeviceLock Content Security Server. Users can install/uninstall DeviceLock Content Security Server, connect to it using DeviceLock Management Console, change its settings, and run search queries; but they cannot add and remove users to and from the Server Administrators group or change access rights granted to Server Administrators. • **Read-only** - enables read-only access to DeviceLock Content Security Server. Users can connect to DeviceLock Content Security Server using DeviceLock Management Console, run search queries and view settings; but they cannot modify any settings or create a new index for Search Server. • **Shadow Data Access** - to enable access to shadowed data. Users can open, view and download shadow data on search results page and search inside of shadowed files. **Note:** We strongly recommend that members of the Server Administrators group have local administrator privileges. To remove a user or group from the Server Administrators group, under **Users**, select the user or group, and then click **Delete**. *You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them*.

4. Click **OK**.

Task: Change the service startup account or password

Over time, you might need to change the account that you specified as the service startup account for DeviceLock Content Security Server during the installation process. You can also change the password of the service startup account.

To change the service startup account or password

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options.**

   When you select Server Options in the console tree, they are displayed in the details pane.

3. In the details pane, double-click **Service startup account** or right-click **Service startup account** and then click **Properties.**

   The DeviceLock Content Security Server dialog box appears.

4. In the **DeviceLock Content Security Server** dialog box, do the following:

TO DO THIS	FOLLOW THESE STEPS
To change the service startup account	1. In the **Log on as** area, click **Browse**. *The Select User dialog box appears*. 2. In the **Select User** dialog box, in the **Enter the object name to select** box, type the name of the user, and then click **OK**. *The user that you selected is displayed in the This account box in the DeviceLock Content Security Server dialog box*. *We recommend that you use an account that has administrative privileges on all computers running DeviceLock Enterprise Server. In a domain environment, we recommend that you use an account that is a member of the Domain Admins group. Otherwise, you will need to use DeviceLock Certificate authentication*.
To change the service account password	1. In the **Log on as** area, type a new password in the **Password** box. 2. Re-type your new password in the **Confirm password** box.
To assign the Local System account to the server service	• In the **Log on as** area, click **Local System account**. *If the service uses this account, it cannot access DeviceLock Enterprise Server running on a remote computer and must use the DeviceLock Certificate for authentication on it*.

5. Click **OK**.

Task: Install or remove DeviceLock Certificate used to authenticate communications between DeviceLock Content Security Server and DeviceLock Enterprise Server

There can be situations when the user account under which DeviceLock Content Security Server is running cannot access remote DeviceLock Enterprise Server. In these situations, you can use DeviceLock Certificate authentication. To do so, install the same private key of DeviceLock Certificate on DeviceLock Content Security Server and DeviceLock Enterprise Server. For detailed information on DeviceLock Certificates, see "DeviceLock Certificates."

To install or remove DeviceLock Certificate on DeviceLock Content Security Server

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options.**

   When you select Server Options in the console tree, they are displayed in the details pane.

3. In the details pane, double-click **DeviceLock certificate** or right-click **DeviceLock certificate** and then click **Properties.**

   The DeviceLock Content Security Server dialog box appears.

4. In the **DeviceLock Content Security Server** dialog box, do the following:

TO DO THIS	FOLLOW THESE STEPS
To install the private key of DeviceLock Certificate	1. Next to the **Certificate Name** box, click the ellipsis button ... to open the **Select the DeviceLock Certificate file** dialog box and browse for the file to use. 2. In the **Select the DeviceLock Certificate file** dialog box, in the **Look in** list, click the location that contains the certificate file. 3. In the folder list, locate and open the folder that contains the certificate file. 4. Click the file, and then click **Open**. *The certificate name now appears in the Certificate Name box of the DeviceLock Content Security Server dialog box*.
To remove the private key of DeviceLock Certificate	• Next to the **Certificate Name** box, click **Remove**.

5. Click **OK**.

Task: Change the TCP port that is used to connect to DeviceLock Management Console

Over time, you might need to change the TCP port that DeviceLock Content Security Server uses to connect to DeviceLock Management Console.

To change the TCP port that is used to connect to DeviceLock Management Console

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options.**

When you select Server Options in the console tree, they are displayed in the details pane.

3. In the details pane, double-click **TCP port** or right-click **TCP port** and then click **Properties.**

   The DeviceLock Content Security Server dialog box appears.

4. In the **DeviceLock Content Security Server** dialog box, in the **Connection Settings** area, do one of the following:
   - Click **Dynamic ports** to configure DeviceLock Content Security Server to use a dynamic port.
     - OR -
   - Click **Fixed TCP port** to configure DeviceLock Content Security Server to use a static port. Next, type the port number in the **Fixed TCP port** box.
     By default, DeviceLock Content Security Server communicates over TCP port 9134.
5. Click **OK**.

Configuring Full-Text Search Settings for Search Server

Full-text search settings are related to full-text search and apply only to the Search Server component of DeviceLock Content Security Server.

During the installation of DeviceLock Content Security Server, you can only install the Search Server licenses. Use DeviceLock Management Console to define the full set of Search Server configuration options.

With DeviceLock Management Console, you can perform the following configuration tasks:

- Install the required number of Search Server licenses.
- Specify DeviceLock Enterprise Server(s) whose data will be indexed for full-text search.
- Specify the location of the full-text index.
- Allow or disallow the index to include textual information from binary data.
- Configure the full-text indexing schedule.
- Configure a schedule for merge operations.
- Rebuild the full-text index immediately.
- Update the existing index immediately.
- Monitor and refresh the status of the current indexing activity.

Task: Install the required number of Search Server licenses

There is a special Search Server license which you must purchase for DeviceLock Content Security Server. You can use the same license on an unlimited number of computers running DeviceLock Content Security Server.

The Search Server licensing model is based on the number of log entries to be indexed for full-text search. Each license allows Search Server to index 1,000 entries from the shadow logs (Shadow Log and Deleted Shadow Data Log), and 5,000 entries from every other log (Audit Log, Server Log, and Monitoring Log).

Depending on the actual number of log entries on your DeviceLock Enterprise Servers, you can purchase as many licenses as required. If you use several licenses for Search Server, it can index as many log entries as the combined licenses allow. The trial period for DeviceLock Content Security Server is 30 days. During the trial period, Search Server can index 2,000 entries from the shadow logs and 10,000 entries from every other log. You can always purchase and install additional Search Server licenses.

To install Search Server licenses

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.

   When you select Search Server Options in the console tree, they are displayed in the details pane.

3. In the details pane, double-click **Search Server License(s)** or right-click **Search Server License(s)** and then click **Properties.**

   The DeviceLock Content Security Server dialog box appears.

4. In the **DeviceLock Content Security Server** dialog box, click **Load License(s)** to browse for the license file.
5. In the **Select the DeviceLock license file** dialog box, in the **Look in** list, click the location that contains the license file.
6. In the folder list, locate and open the folder that contains the license file.
7. Click the file, and then click **Open**.

   After you have successfully loaded your license files, you can view the license information summary where Total license(s) displays the total number of purchased licenses while Used license(s) displays the number of licenses currently in use for indexing of textual log data on DeviceLock Enterprise Server.

   You can install as many licenses as required to suit your organization's needs. To do this, add them one by one.

8. Click **OK**.

Task: Specify DeviceLock Enterprise Server(s) whose data will be indexed for full-text search

To start the process of creating the full-text index, you must specify DeviceLock Enterprise Server(s) whose data will be indexed. Search Server starts the indexing process automatically as soon as you specify DeviceLock Enterprise Server(s).

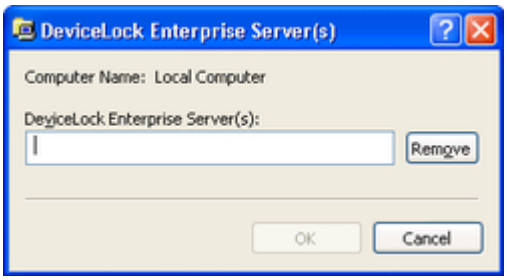
To specify DeviceLock Enterprise Server(s)

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.

   When you select Search Server Options in the console tree, they are displayed in the details pane.

3. In the details pane, double-click **DeviceLock Enterprise Server(s)** or right-click **DeviceLock Enterprise Server(s)** and then click **Properties**.

   The DeviceLock Enterprise Server(s) dialog box appears.



4. In the **DeviceLock Enterprise Server(s)** dialog box, type the IP address or the name of the computer that is running DeviceLock Enterprise Server.

   Multiple computer names or IP addresses must be separated by a semicolon (;).

   Note: Make sure that DeviceLock Enterprise Server is properly installed and accessible to DeviceLock Content Security Server, otherwise its data will not be indexed by Search Server.

   To remove computer names or IP addresses, click **Remove**.

5. Click **OK**.

Task: Specify the location of the full-text index

You can specify where the full-text index will reside. If you do not specify a location, the full-text index is created in the default directory ***%ProgramFiles%\DeviceLock Content Security Server\Index***. Search Server starts the indexing process automatically each time you specify a different location.

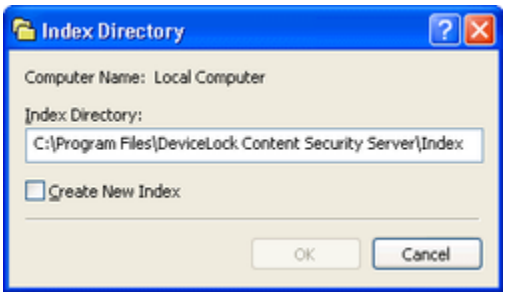
To specify the index location

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.

   When you select Search Server Options in the console tree, they are displayed in the details pane.

3. In the details pane, double-click **Index directory** or right-click **Index directory** and then click **Properties**.

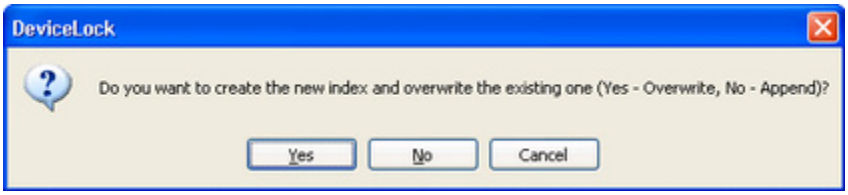
The Index Directory dialog box appears.



4. In the **Index Directory** dialog box, in the **Index Directory** box, type the path that you want to use as your default index location.

   If you want to immediately create a new index, select the **Create New Index** check box.

   If the index already exists at the specified location and you choose to create a new index, the following message box is displayed:



   In the message box, click **Yes** to completely rebuild the full-text index immediately. Click **No** to update the existing full-text index with changes immediately.

5. Click **OK**.

Task: Allow or disallow the index to include textual information from binary data

You can allow or disallow the index to include textual information from binary data.

To enable or disable the extraction of text from binary data

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.

   When you select Search Server Options in the console tree, they are displayed in the details pane.

3. In the details pane, double-click **Extract text from binary** or right-click **Extract text from binary**, and then click **Enable** or **Disable**.

Task: Configure the full-text indexing schedule

Full-text indexing enables the creation and subsequent update of the full-text index.

You can schedule the indexing process to automatically start at a predetermined interval. The full-text indexing schedule is configured based on the indexing interval. The indexing

interval specifies the time interval, in minutes, between the end of one indexing process and the start of the next indexing process. The default indexing interval is 60 minutes.

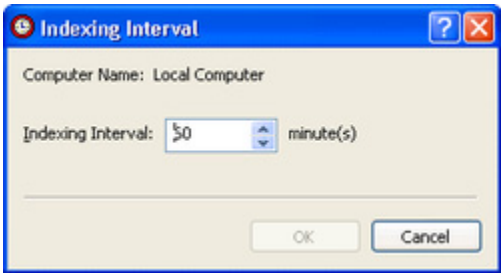
To configure the full-text indexing schedule

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.

   When you select Search Server Options in the console tree, they are displayed in the details pane.

3. In the details pane, double-click **Indexing interval** or right-click **Indexing interval** and then click **Properties**.

   The Indexing Interval dialog box appears.



4. In the **Indexing Interval** dialog box, in the **Indexing Interval** box, type or select the number of minutes for the indexing interval.
5. Click **OK**.

Task: Configure a schedule for merge operations

Merge operations are used to combine temporary indexes into a permanent master index that is used for search queries. You can schedule the merging process to start at a predetermined interval. The schedule is configured based on the merge interval. The merge interval determines how often, in minutes, Search Server combines temporary indexes into a permanent master index, or in other words, updates the master index with new data during an indexing operation. By default, the merge is performed every 10 minutes. The range of values that you can specify is 1 to 1,000,000.

When specifying the merge interval, consider the following:

- A small merge interval will result in faster updates of the master index.
- You cannot perform full-text searches while merging is in progress.

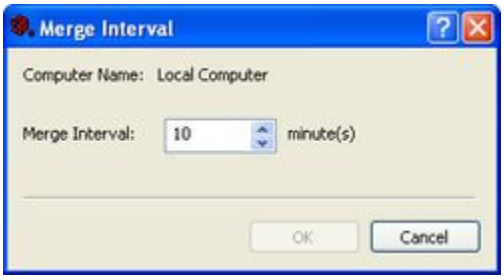
To configure a schedule for merge operations

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Option**s.

   When you select Search Server Options in the console tree, they are displayed in the details pane.

3. In the details pane, double-click **Merge Interval** or right-click **Merge Interval** and then click **Properties**.

   The Merge Interval dialog box appears.



4. In the **Merge Interval** dialog box, in the **Merge Interval** box, type or select the number of minutes for the merge interval.
5. Click **OK**.

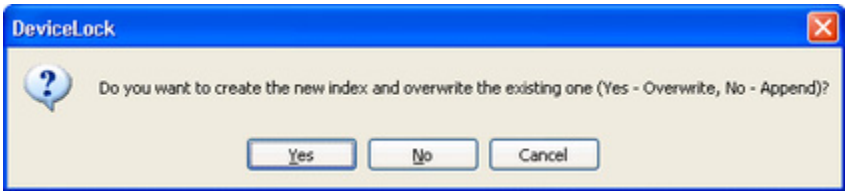
Task: Rebuild the full-text index immediately

You can completely rebuild the full-text index immediately.

To rebuild the full-text index immediately

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, right-click **Search Server**, and then click **Create New Index**.

   If the index already exists and you choose to create a new index, the following message box is displayed:



   In the message box, click **Yes** to completely rebuild the full-text index immediately. Click **No** to update the existing full-text index with changes immediately.

Task: Update the existing index immediately

If new data is added to DeviceLock Enterprise Server and you want to update the existing full-text index with these changes immediately, use the following procedure:

To update the existing index immediately

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, right-click **Search Server**, and then click **Index Now**.

   During an update operation, Search Server does not perform a full rebuild of the index. It indexes only new data on DeviceLock Enterprise Server in order to add new

index entries to the existing index.

Task: Monitor and refresh the status of the current indexing activity

Full-text indexing operations can be time-consuming and resource-intensive. Search Server lets you monitor the progress of the indexing operations that are currently being executed.

The indexing process happens in two stages. In the first stage, Search Server extracts significant words from shadow copies and log records and saves them to temporary indexes for each specified DeviceLock Enterprise Server. For each temporary index, Search Server processes 1,000 records from each log.

In the second stage, when either the number of temporary indexes becomes equal to 50 or 10 minutes pass, all temporary indexes are combined into a permanent master index that is used for search queries. The process of combining temporary indexes into a master index is called ***merging***.

Search Server provides indexing and merging-related progress and status indicators.

Indexing progress and status indicators

You can control the indexing process on each specified DeviceLock Enterprise Server by watching its status and progress counter. The status indicator shows the status of the indexing operation. The following table shows possible status values and their descriptions.

STATUS VALUE	DESCRIPTION
Idle	Indexing is not performed
Waiting	Waiting for indexing to begin
Indexing <*log_name*>	Indexing is in progress

The progress counter shows the percentage complete of the indexing process.

Merging-related progress and status indicators

You can control the merge process by watching its status and progress counter. The status indicator shows the status of the merge operation. The following table shows possible status values and their descriptions.

STATUS VALUE	DESCRIPTION
Idle	The merge is not performed
Merging	The merge is in process
Defragmenting	Compressing (optimizing) the index. Compressing the index optimizes the index structure, removing obsolete data and defragmenting search structures for better performance.

The progress counter shows the percentage complete of the merge process.

To monitor and refresh the status of the current indexing activity

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Search Server**.
2. Under **Search Server**, select **Current Activity**.

   When you select Current Activity in the console tree, indexing and merging-related progress and status indicators are displayed in the details pane.

   Because the status of the current indexing and merging-related operations is not updated automatically, you need to perform a refresh operation.

   To perform a refresh operation, do one of the following:

   - In the console tree, right-click **Current Activity**, and then click **Refresh**.
     - OR -
   - In the console tree, select **Current Activity**, and then click **Refresh** on the toolbar.
     - OR -
   - In the console tree, select **Current Activity**. In the details pane, in the **Name** column, right-click any name of DeviceLock Enterprise Server or **Merge Index**, and then click **Refresh**.
     - OR -
   - In the console tree, select **Current Activity**. In the details pane, select the name of any DeviceLock Enterprise Server or **Merge Index**, and then click **Refresh** on the toolbar.

Using Search Server

Using Search Server involves the following:

- Performing a full-text search operation
- Working with search results

Performing a Full-Text Search Operation

With Search Server, you can locate every occurrence of a word or phrase in the DeviceLock Enterprise Server database. Because most searches return a large number of results, you can set search options to fine-tune and optimize your search. Search options specify how search results should be returned.

Using search options, you can specify

- How many search results to return per page.
- How to filter the search results that are retrieved. Search results can be filtered by date and log. For example, you can limit the number of results to those within a certain date range and to those that are retrieved from certain logs.

Here are some notes to consider when using full-text search:

- Searches are not case sensitive.
- Stemming is enabled by default. Stemming extends a search to cover grammatical variations on a word. E.g. **applied** would also retrieve **applying**, **applies**, and **apply**. Stemming is supported for next languages: English, French, German, Italian, Portugal, Russian, and Spanish.
- You can search for words and phrases and use familiar wildcards such as asterisks (*) and question marks (?) in search queries. An asterisk (*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity. To search for a specific phrase, enclose the phrase in double quotes. To search for multiple words, separate each word with a space.

  The following table shows the search items, examples, and results of these types of searches.

SEARCH ITEM	EXAMPLE	RESULTS
Single word	price	Results that contain the word ***price.*** You will also find its grammatical variations, such as ***prices***, ***priced*** and so on.
Phrase	confidential information	Results that contain both of the individual words ***confidential*** and ***information***, instead of the exact phrase.
	"confidential information"	Results that contain the exact phrase ***confidential information***.
Wildcard expression	te?t	Results that contain ***test***, ***text***, and so on.
Wildcard expression	mone*	Results that contain ***money***, ***monetary***, and so on.
Wildcard expression	*air	Results that contain ***air***, ***fair***, ***impair***, ***affair***, and so on.
Wildcard expression	"* assets"	Results that contain ***monetary assets***, ***liquid assets***, ***fixed assets***, ***current assets***, and so on.

Moreover, Search Server supports advanced syntax in search queries.

CHARACTER	MEANING	DESCRIPTION
=	any single digit	**N===** would match **N123** but not **N1234** or **Nabc**.

CHARACTER	MEANING	DESCRIPTION
-	exclude	Put - (minus) in front of a word or phrase to exclude it. E.g. **–"*monetary assets*"**
%	fuzzy search	Fuzzy searching will find a word even if it is misspelled. The number of % characters you add determines the number of differences ignored when searching for a word. The position of the % characters determines how many letters at the start of the word have to match exactly. Fuzzy searching can be useful when you are searching text that may contain typographical errors. E.g. **inf%%ormation** – would find a word that begins with **inf** and has at most two differences between it and **information**.
#	phonic search	Phonic searching looks for a word that sounds like the word you are searching for and begins with the same letter. Phonic searching is somewhat slower than other types of searching and tends to make searches over-inclusive. For the English language only. E.g. **#smith** would find **smithe** and **smythe**.
&	synonym search	Synonym searching finds synonyms of a word that you include in a search request. For the English and Russian languages only. E.g. **fast&** would also find **quickly**.
~~	numeric range	A numeric range search is a search for any numbers that fall within a range. To add a numeric range component to a search request, enter the upper and lower bounds of the search separated by ~~. A numeric range search includes the upper and lower bounds. Decimal points and commas are treated as spaces and minus signs are ignored. E.g. **500~~1000** would find a text containing a number between **500** and **1000**.
:	variable term weighting	By default all words in a request count equally in counting hits. However, you can change this by specifying the relative weights for each term in your search request. E.g. **money:5 information:1** would retrieve the same documents as **money information** but the Search Server would weight **money** five times as heavily as **information** when sorting the results.

CHARACTER	MEANING	DESCRIPTION
##	regular expression	Regular expression searching provides a way to search for advanced combinations of characters. A regular expression included in a search request must be quoted and must begin with ##. The TR1 implementation of regular expressions is used. For more information, please refer to the Microsoft's on-line article: http://msdn.microsoft.com/en-us/library/bb982727.aspx. A regular expression must match a single whole word. Only letters are searchable. No case or other conversion is done on regular expressions, so a regular expression must match the case of the information stored in the index. A regular expression is like the * wildcard character in its effect on search speed: the closer to the front of a word the expression is, the more it will slow searching. The = wildcard, which matches a single digit, is faster than regular expressions for matching patterns of numbers. E.g. **##10[0-9]+**

To perform a search operation

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Search Server**.
2. Under **Search Server**, select **Search Page**.

   The search page is displayed in the details pane.

3. On the search page, in the **Search** box, type the word or phrase you want to find. To set search options, click **Options** and then do the following:
   - To specify the number of search results to display per page, in the **Display**…**results per page** list, click any of the following options: **10**, **20**, **30**, **50**, **100**. The default number of returned results is 20.
   - To limit the scope of the search to specific data stores, select the appropriate check boxes under **Limit results to the following logs**.

     By default, Search Server retrieves search results from the Audit Log, Shadow Log, and Deleted Shadow Data Log.
   - To filter search results by date, specify a date range that limits the data retrieved from the data sources. To do so, set the following date parameters:

PARAMETER	DESCRIPTION
From	Specifies the beginning of the date range in which to search. Possible values: **First Record** or **Records On**. The default value is **First Record**.

PARAMETER	DESCRIPTION
	First Record causes Search Server to retrieve data starting with the first record written to the log. **Records On** causes Search Server to retrieve data that was written starting with a specific date.
To	Specifies the end of the date range in which to search. Possible values: **Last Record** or **Records On**. The default value is **Last Record**. **Last Record** causes Search Server to retrieve data ending with the last record written to the log. **Records On** causes Search Server to retrieve data that was written ending with a specific date.

If you set the date parameters to **Records On**, click in the **From** and **To** boxes to display the calendar. In the calendar, click to select the day. You can use single arrows (**<>**) to change what month you view and double arrows (**<<>>**) to change what year you view.

4. Click **Search**.

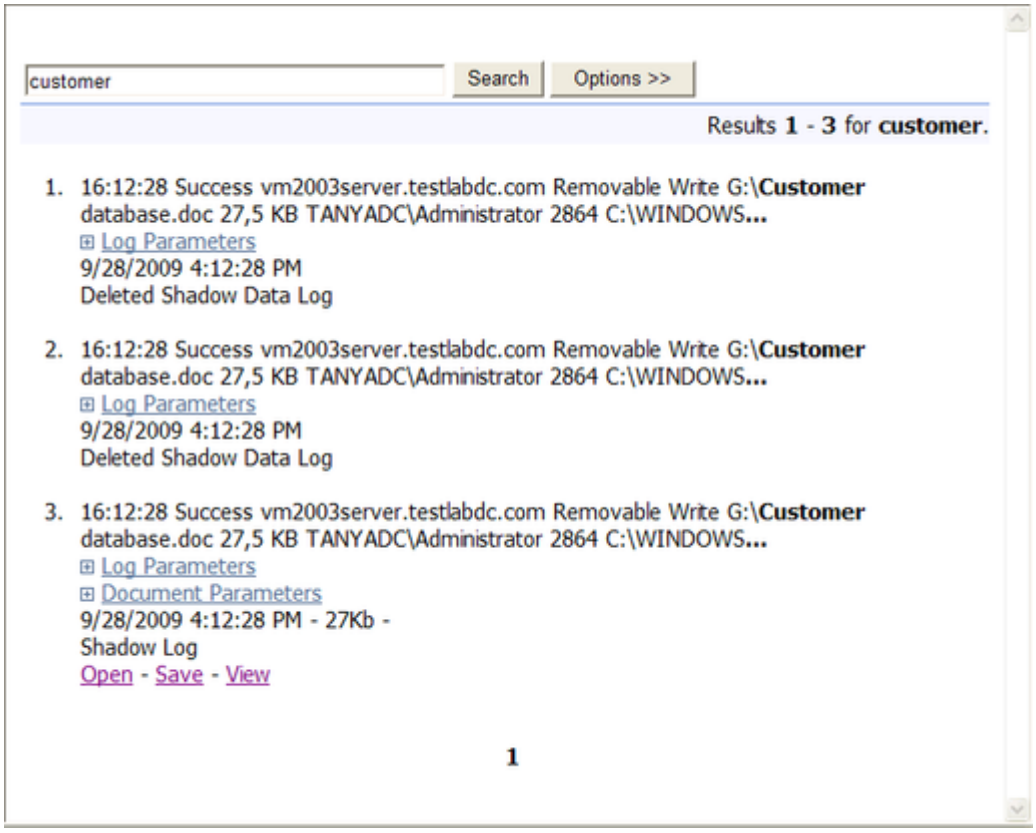
Working with Search Results

Working with search results involves the following:

- Interpreting search results
- Manipulating search results retrieved from the Shadow Log

Interpreting search results

After you enter search criteria and submit you search, Search Server returns the search results page which looks like this.

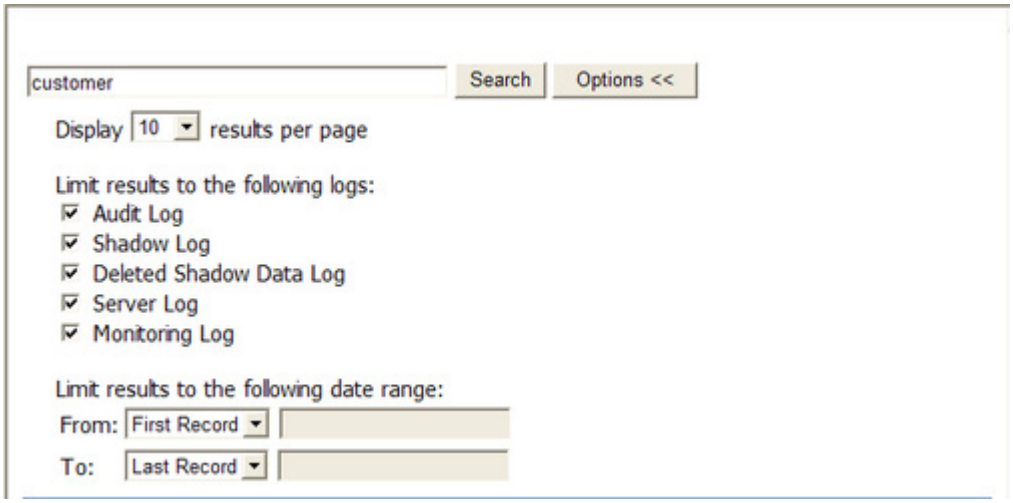

customer
Search
Options >>
Results 1 - 3 for customer.
1. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
2. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
3. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
Document Parameters
9/28/2009 4:12:28 PM - 27Kb -
Shadow Log
Open - Save - View
1

The search results page is divided into the following viewing areas:

- **Search query** – displays the search criteria you entered.
- **Statistics bar** – shows the number of results displayed on the current search results page.
- **Search results** – displays a numbered list of items containing information that matched the search criteria you entered.
- **Results navigator** – shows how many results pages are returned and allows you to navigate from page to page.

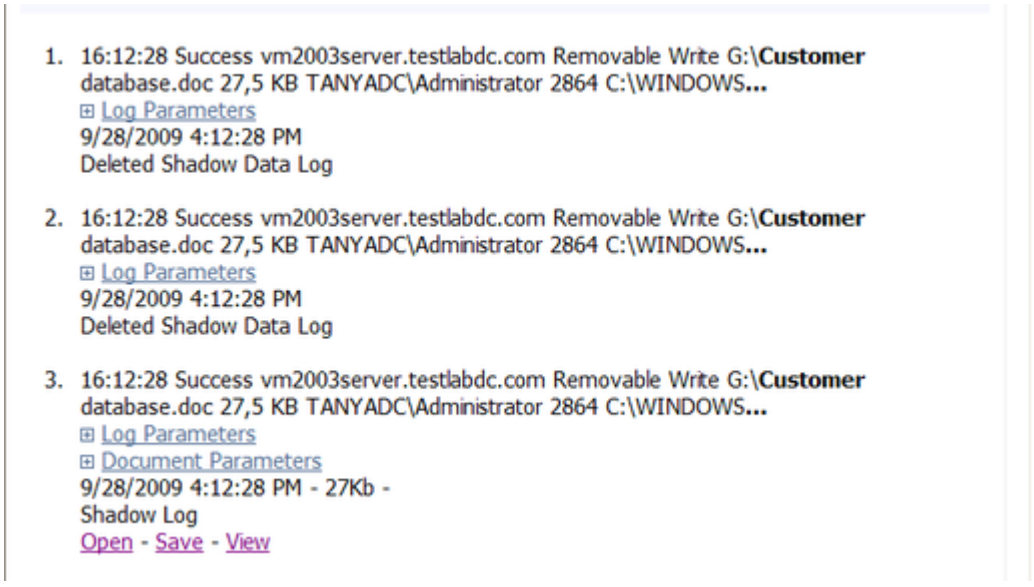
Each of these areas is described in more detail below.

Search query
This area is located at the top of the search results page. Click **Options** to view additional search criteria you specified.



Statistics bar
This area is located immediately above the search results area and looks like this.

Search results
This area is located below the search query area and statistics bar and looks like this.


1. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
2. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
3. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
Document Parameters
9/28/2009 4:12:28 PM - 27Kb -
Shadow Log
Open - Save - View

A search result includes the following:

- ***Snippets*** – portions of text containing highlighted query words (bold font). These snippets allow you to see the context in which the query words were found. The search results page displays only the first three snippets per search result.

- ***Log Parameters*** – summary information retrieved from the log for this search result. Click the plus sign (**+**) to expand **Log Parameters** and view this information. This information is different, depending on the log type.

  Note: If an entry in a log has an empty field, this field is not displayed in **Log Parameters**.

  The following information is displayed in **Log Parameters** for a result retrieved from the Audit Log:

  - **Received Date/Time** – the date and time when the event was received by DeviceLock Enterprise Server.
  - **Type** – the class of the event, either **Success** for allowed access or **Failure** for denied access. This value matches the value in the **Type** column of the server's Audit Log Viewer.
  - **Computer** – the name of the computer from which the Audit Log was received. This value matches the value in the **Computer** column of the server's Audit Log Viewer.
  - **Date/Time** – the date and time when the event was received by DeviceLock Service. This value matches the value in the **Date/Time** column of the server's Audit Log Viewer.
  - **Source** – the type of device or protocol involved. This value matches the value in the **Source** column of the server's Audit Log Viewer.
  - **Action** – the user's activity type. This value matches the value in the **Action** column of the server's Audit Log Viewer.
  - **Name** – the name of the object (file, USB device, etc.). This value matches the value in the **Name** column of the server's Audit Log Viewer.
  - **Information** – other device-specific information for the event, such as the access flags, device names, and so on. This value matches the value in the **Information** column of the server's Audit Log Viewer.
  - **Reason** – the cause of the event. This value matches the value in the **Reason** column of the server's Audit Log Viewer.
  - **User** – the name of the user associated with this event. This value matches the value in the **User** column of the server's Audit Log Viewer.
  - **PID** – the identifier of the process associated with this event. This value matches the value in the **PID** column of the server's Audit Log Viewer.
  - **Process** – the fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path. This value matches the value in the **Process** column of the server's Audit Log Viewer.
  - **Event** – the number identifying the event type. This value matches the value in the **Event** column of the server's Audit Log Viewer.

  The following information is displayed in **Log Parameters** for a result retrieved from the Shadow Log or Deleted Shadow Data Log:

  - **Received Date/Time** – the date and time when the data was received by DeviceLock Enterprise Server.
  - **Status** – the status of the record. The **Success** status indicates that data is successfully logged; the **Incomplete** status indicates that data is possibly not completely logged while the **Failed** status is given to shadow copies of files checked by Content-Aware Rules and whose transmission was blocked. This value matches the value in the **Status** column of the server's Shadow Log Viewer.

- **Computer** – the name of the computer from which the Shadow Log was received. This value matches the value in the **Computer** column of the server's Shadow Log Viewer.
- **Date/Time** – the date and the time when the data was transferred. This value matches the value in the **Date/Time** column of the server's Shadow Log Viewer.
- **Source** – the type of device or protocol involved. This value matches the value in the **Source** column of the server's Shadow Log Viewer.
- **Action** - the user's activity type. This value matches the value in the **Action** column of the server's Shadow Log Viewer.
- **File Name** - the original path to the file or the auto-generated name of the data that originally was not a file (such as CD/DVD/BD images, data written directly to the media or transferred through the serial/parallel ports). This value matches the value in the **File Name** column of the server's Shadow Log Viewer.
- **File Size** – the size of the data. This value matches the value in the **File Size** column of the server's Shadow Log Viewer.
- **User** – the name of the user who transferred the data. This value matches the value in the **User** column of the server's Shadow Log Viewer.
- **PID** – the identifier of the process used to transfer the data. This value matches the value in the **PID** column of the server's Shadow Log Viewer.
- **Process** – the fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path. This value matches the value in the **Process** column of the server's Shadow Log Viewer.

The following information is displayed in **Log Parameters** for a result retrieved from the Server Log:

- **Type** – the class of the event: **Success**, **Information**, **Warning** or **Error**. This value matches the value in the Server Log Viewer's **Type** column.
- **Date/Time** – the date and time when the event occurred. This value matches the value in the Server Log Viewer's **Date/Time** column.
- **Event** – the number identifying the event type. This value matches the value in the Server Log Viewer's **Event** column.
- **Information** – event-specific information, such as error/warning descriptions, names and values of changed parameters, and so on. This value matches the value in the Server Log Viewer's **Information** column.
- **Server** – the name of the server where the event occurred. This value matches the value in the Server Log Viewer's **Server** column.
- **Record N** – the record number. This value matches the value in the Server Log Viewer's **Record N** column.

The following information is displayed in **Log Parameters** for a result retrieved from the Monitoring Log:

- **Type** – the class of the event: **Success**, **Information**, **Warning** or **Error**. This value matches the value in the **Type** column of the server's Monitoring Log Viewer.
- **Date/Time** – the date and time when the event occurred. This value matches the value in the **Date/Time** column of the server's Monitoring Log Viewer.
- **Event** – the number identifying the event type. This value matches the value in the **Event** column of the server's Monitoring Log Viewer.

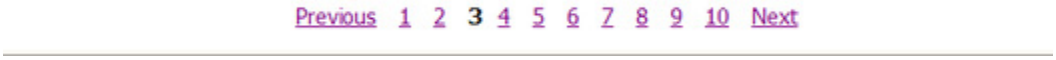
- **Task Name** – the name of the task responsible for this event. Can be empty if the event does not link to any task. This value matches the value in the **Task Name** column of the server's Monitoring Log Viewer.
- **Computer Name** – the name of the computer belonging to the task that is responsible for this event. Can be empty if the event does not link to the computer. This value matches the value in the **Computer Name** column of the server's Monitoring Log Viewer.
- **Information** – event-specific information, such as status, error, warning, and so on. This value matches the value in the **Information** column of the server's Monitoring Log Viewer.
- **Server** – the name of the server where the event occurred. This value matches the value in the **Server** column of the server's Monitoring Log Viewer.
- **Record N** – the record number. This value matches the value in the **Record N** column of the server's Monitoring Log Viewer.

- ***Document Parameters*** – summary information retrieved from the document properties for this search result. This information is retrieved randomly and is displayed only for shadow copies. Click the plus sign (**+**) to expand **Document Parameters** and view this information. This information is different, depending on the file type. For example, the following information is displayed in **Document Parameters** for a shadow copy of a Word document:
  - **Application:** Microsoft Office Word.
  - **Author:** the name of the user who created the document.
  - **Created:** the date and time when the document was created.
  - **LastSaved:** the date and time when the document was last saved.
  - **LastSavedBy:** the name of the user who last saved the document.
  - **RevisionNumber:** the number of times the document has been saved.
  - **Template:** the name of the template attached to the document.
  - **Title:** the name of the document.
  - **TotalEditingTime:** the number of minutes that the document has been opened for making changes since it was created.
- ***The date and time when the log entry was created.***
- ***The size of the log entry***. This value is displayed only for shadow copies retrieved from the Shadow Log.
- ***The name of the log in which matches of the query occurred.***
- ***Open, Save and View links*** – allow you to access and manipulate the search results (shadow copies) retrieved from the Shadow Log. For detailed information on how to manipulate shadow copies, see "Manipulating search results retrieved from the Shadow Log."

Note: If your search produced no results, the search results page displays a message indicating that no matches were found.

Results navigator

This area is located at the bottom of the search results page and looks like this.



To move forward or backward through your results, click **Next** or **Previous** or click the page number.

Manipulating search results retrieved from the Shadow Log

You can perform the following operations on results retrieved from the Shadow Log:

- Open a shadow copy of a file in its native application.
- Save a shadow copy of a file to any local or network location.
- Open and save a shadow copy of a file using the built-in viewer.

Below are step-by-step instructions demonstrating how to perform these operations.

To open a shadow copy of a file in its native application

1. Perform your search.
2. On the search results page, click **Open** under the desired search result.

   The shadow copy of the file opens in its native application.

   If there is no native application, the Open With dialog box appears. Use this dialog box to choose the program with which to open the file.

   If you open the shadow copy of a file captured from the Parallel port device type, it always opens in the built-in DeviceLock Printer Viewer.

   DeviceLock Printer Viewer is able to display a shadowed printed document in the PostScript and native print spooler format, send it to the printer again, or save it as a graphics file (such as BMP, GIF, JPEG, PNG, EMF or TIFF). The following print spooler formats are supported: PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, GDI printing (ZjStream) and EMF Spooled Files.

To save a shadow copy of a file to any local or network location

1. Perform your search.
2. On the search results page, click **Save** under the desired search result.

   The Save As dialog box appears.

3. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the shadow copy.
4. In the **File name** box, type the file name you want.
5. Click **Save**.

   If the data was transferred by the user as a file, it is stored in the shadow log as a file and can be saved to the local computer as a file too.

When a user has written data to a CD/DVD/BD disk, all data is stored in the shadow log as a single CD/DVD/BD image (one image per each written CD/DVD/BD disk or session) in the CUE format.

CD/DVD/BD images as well as other data that originally was not transferred as files (direct media access or serial/parallel ports transfer), have auto-generated names based on the action's type, drive's letter or device's name and time/date (for example, direct_write(E:) 19:18:29 17.07.2006.bin).

Each CD/DVD/BD image is saved to the local computer as two files: the data file with the .bin extension (for example, direct_write(E_) 19_18_29 17_07_2006.bin) and the cue sheet file that has the same name as its data file with the .cue extension (for example, direct_write(E_) 19_18_29 17_07_2006_bin.cue). Both these files are necessary to open the CD/DVD/BD image in the external application that supports the CUE format (such as Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO and many others).

To open and save a shadow copy of a file using the built-in viewer

1. Perform your search.
2. On the search results page, click **View** under the desired search result.

   The shadow copy opens in the built-in viewer.

3. In the built-in viewer, click any of the following viewing options:
   - **Hex** Displays data in hex as well as in words.
   - **Autodetect Text** Enables the auto-detection of encoding for text and displays data in textual format only.
   - **ANSI Text** Specifies ANSI encoding for text and displays data in textual format only.
   - **UTF-16 Text** Specifies Unicode UTF-16 encoding for text and displays data in textual format only.
   - **UTF-16BE Text** Specifies Unicode UTF-16 (Big Endian) encoding for text and displays data in textual format only.

   To save the file, click **Save** to open the **Save As** dialog box. In the **Save As** dialog box, do the following:
   - In the **Save in** box, browse to the location where you want to save the file.
   - In the **File name** box, type the file name you want.
   - Click **Save**.
4. Click **Close** to close the viewer.

DeviceLock Group Policy Manager

Overview

In addition to the standard way of managing permissions via DeviceLock Management Console, DeviceLock also provides you with a more powerful mechanism – settings can be changed and deployed via Group Policy in an Active Directory domain. System administrators can use policies to control DeviceLock's configurations from a single location on a network – no matter how large the network.

Group Policy enables policy-based administration that uses Active Directory. Group Policy uses directory services and security group membership to provide flexibility and support extensive configuration information. Policy settings are created using the Microsoft Management Console (MMC) snap-in for Group Policy.

Tighter integration into Active Directory is a very important function of DeviceLock. It makes DeviceLock's management and deployment easier for large networks and more convenient for system administrators.

Integration with Active Directory eliminates the need to install more third-party applications for centralized management and deployment. DeviceLock does not need to have its own server-based component to control the entire network, instead it uses standard functions provided by Active Directory.

Via Group Policy it is possible to:

- Install DeviceLock Service on all the computers on a network, even those that are not currently running and new computers that are just connecting to the network.
  For more information regarding DeviceLock Service deployment, see "Installation via Group Policy."

- Control and configure DeviceLock Service on a large number of computers in different domains/organizational units simultaneously.
  Even if some computers are not currently running or they are new computers that are just connecting to the network, they are included in DeviceLock's automatic deployment of predefined settings.

- View the policy currently being applied and predict what policy would be applied.
  For more information, see "Using Resultant Set of Policy (RSoP)."

Note: In order to manage DeviceLock via Group Policy, you must have Active Directory properly installed and configured. For more information about installing and configuring Active Directory, please refer to the related Microsoft documentation.

Applying Group Policy

Policy is applied when the computer starts up. When a user turns on the computer, the system applies DeviceLock's policy.

Policy can be optionally reapplied on a periodic basis. By default, policy is reapplied every 90 minutes. To set the interval at which policy will be reapplied, use the Group Policy Object Editor. For more information, please refer to the Microsoft Knowledge Base: http://support.microsoft.com/kb/203607.

Policy can also be reapplied on demand. To refresh the current policy settings immediately on Windows XP and later, administrators can call the ***gpupdate.exe /force*** command-line utility provided by Microsoft. On Windows 2000, administrators can call another command-line utility provided by Microsoft: ***secedit /refreshpolicy machine_policy /enforce***.

When applying policy, the system queries the directory service for a list of Group Policy Objects (GPOs) to process. Each GPO is linked to an Active Directory container to which the computer or user belongs. By default, the system processes the GPOs in the following order: local, site, domain, then organizational unit. Therefore, the computer receives the policy settings of the last Active Directory container processed.

When processing the GPO, the system checks the access-control list (ACL) associated with the GPO. If an access-control entry (ACE) denies the computer access to the GPO, the system does not apply the policy settings specified by the GPO. If the ACE allows access to the GPO, the system applies the policy settings specified by the GPO.

Standard GPO Inheritance Rules

Any unconfigured settings anywhere in a GPO can be ignored since they are not inherited down the tree; only configured settings are inherited. There are three possible scenarios:

- A parent has a value for a setting, and a child does not.
- A parent has a value for a setting, and a child has a non-conflicting value for the same setting.
- A parent has a value for a setting, and a child has a conflicting value for the same setting.

If a GPO has settings that are configured for a parent Organizational Unit, and the same policy settings are unconfigured for a child Organizational Unit, the child inherits the parent's GPO settings. That makes sense.

If a GPO has settings configured for a parent Organizational Unit that do not conflict with a GPO on a child Organizational Unit, the child Organizational Unit inherits the parent GPO settings and applies its own GPOs as well.

If a GPO has settings that are configured for a parent Organizational Unit that conflict with the same settings in another GPO configured for a child Organizational Unit, then the child Organizational Unit does not inherit that specific GPO setting from the parent Organizational Unit. The setting in the GPO child policy takes priority, although there is one case in which this is not true.

If the parent disables a setting and the child makes a change to that setting, the child's change is ignored. In other words, the disabling of a setting is always inherited down the hierarchy.

Starting DeviceLock Group Policy Manager

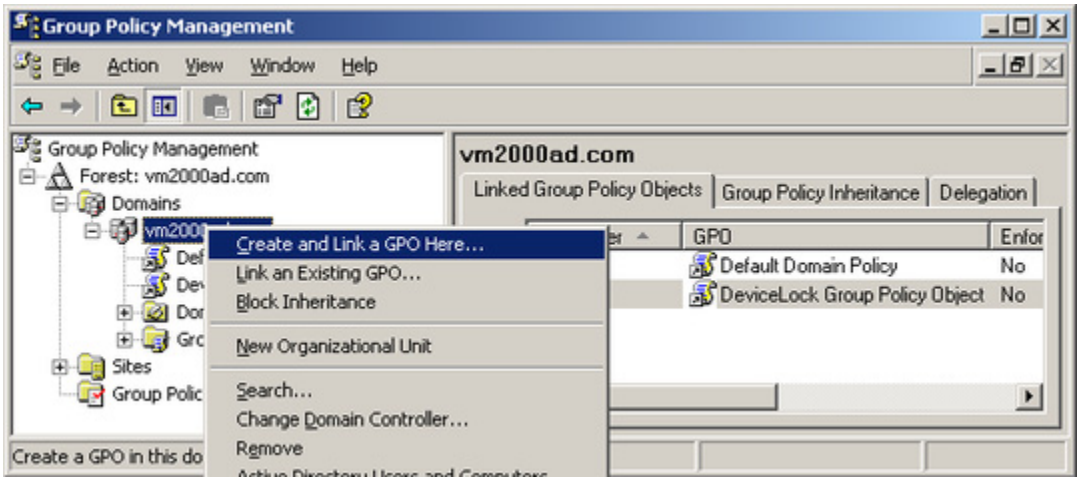
DeviceLock Group Policy Manager integrates into the Windows Group Policy Object (GPO) editor. To use DeviceLock Group Policy Manager on your local PC rather than on the domain controller, you need to have the GPO editor installed locally. We recommend that you install the Group Policy Management Console (GPMC). It can be downloaded from the Microsoft Download Center.

To open DeviceLock Group Policy Manager, you should run the GPO editor first:

1. Start the Group Policy Management snap-in.

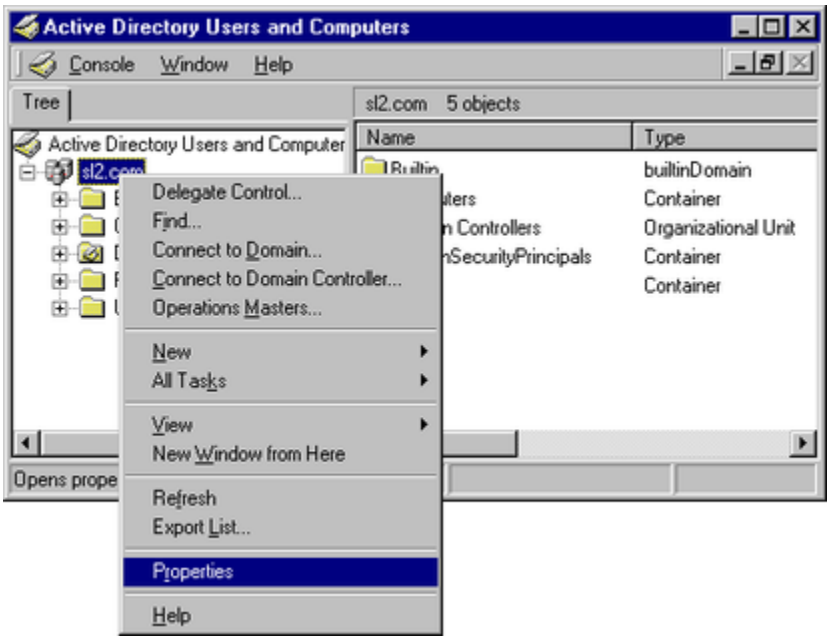
   If the Group Policy Management snap-in is not installed on your computer, you may use the Active Directory Users and Computers snap-in instead.

2. In the console tree, select your domain.

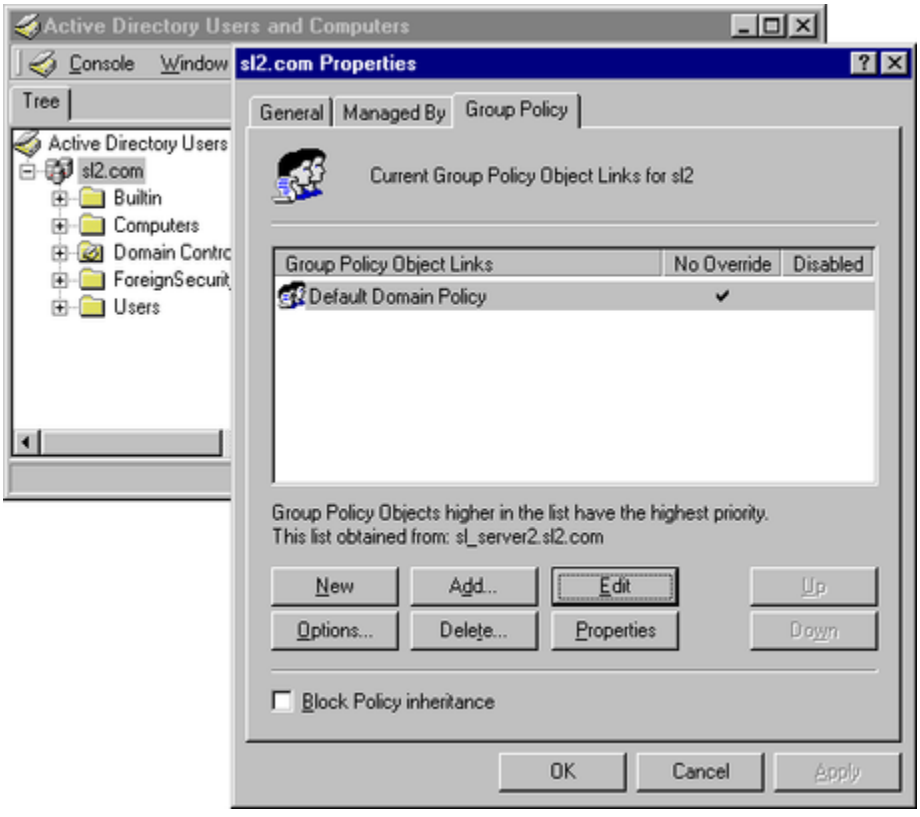


3. Select the group policy object that you need, and then click **Edit** on the context menu available by a right mouse click. If you wish to create a new group policy object, click **Create and Link a GPO Here** on the context menu of the selected domain.

   If you are using the Active Directory Users and Computers snap-in, right-click your domain, then click **Properties**.



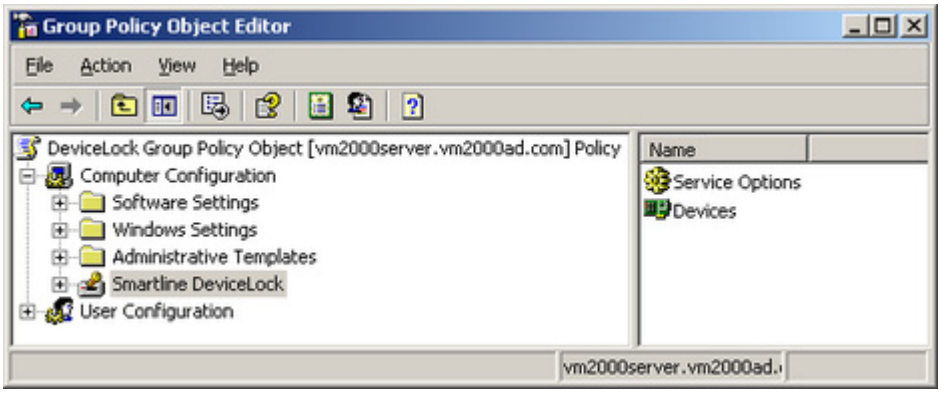
Click the **Group Policy** tab, select the group policy object that you need, and then click **Edit**. If you wish to create a new group policy object, click **New**.



4. Wait until the GPO editor is started.

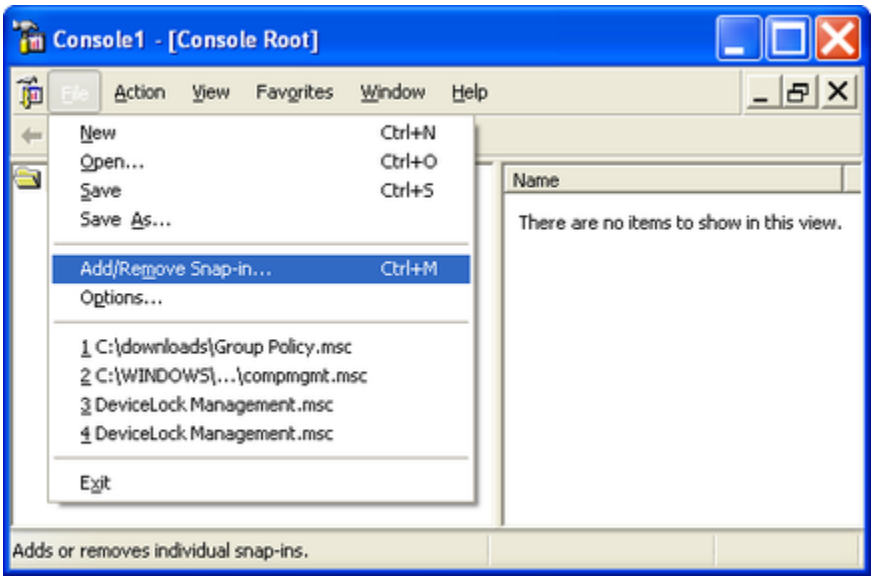
   It may take up to several seconds.

5. Under **Computer Configuration**, select **DeviceLock**.

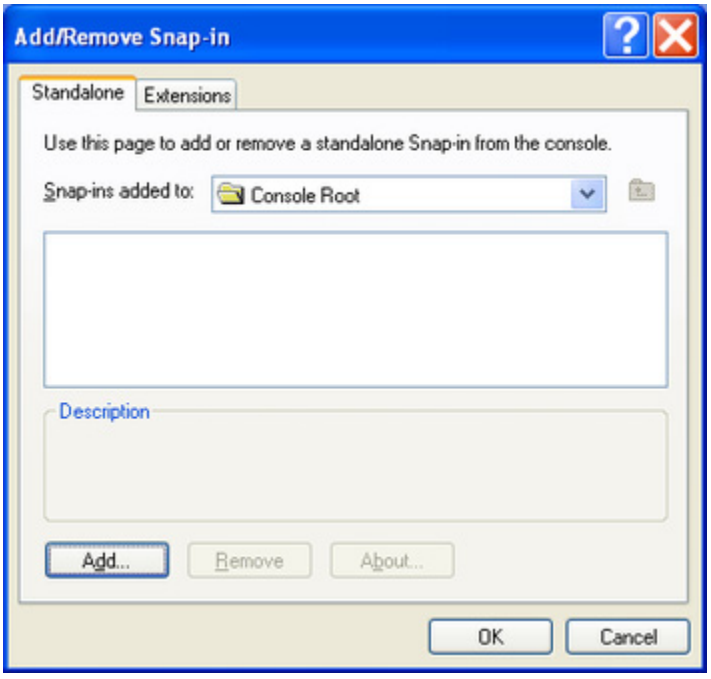


Alternatively, to run the GPO editor you can start MMC and add the Group Policy snap-in manually:

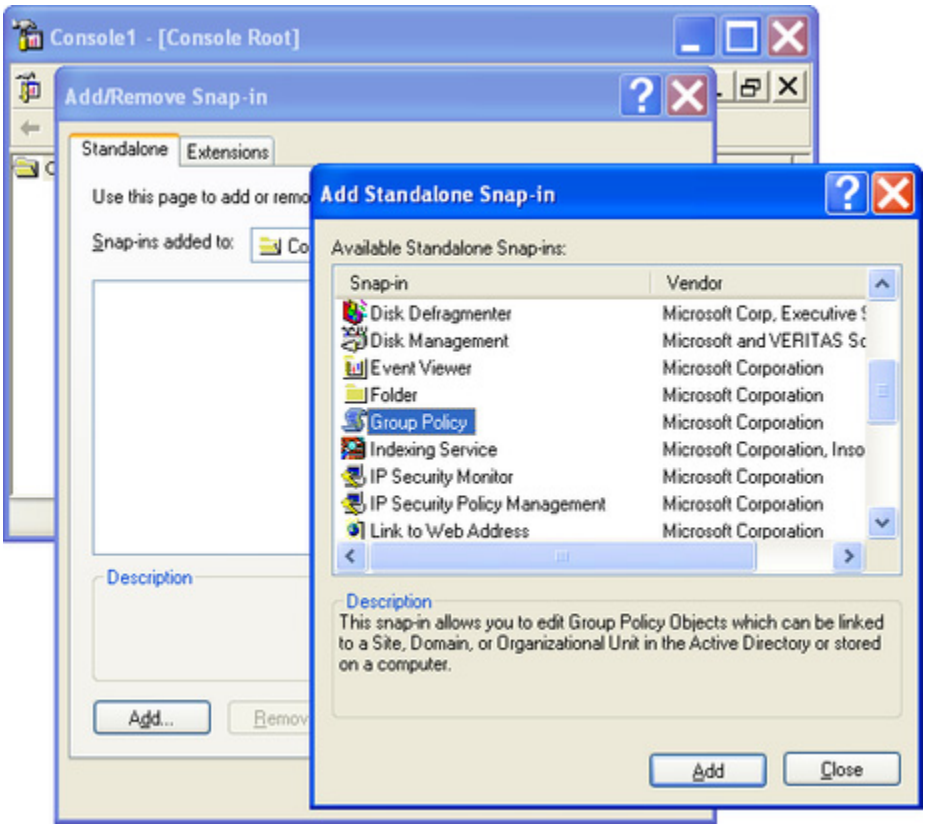
1. Run **mmc** from the command line or use the **Run** menu to execute this command.
2. On the **File** menu, click **Add/Remove snap-in**.



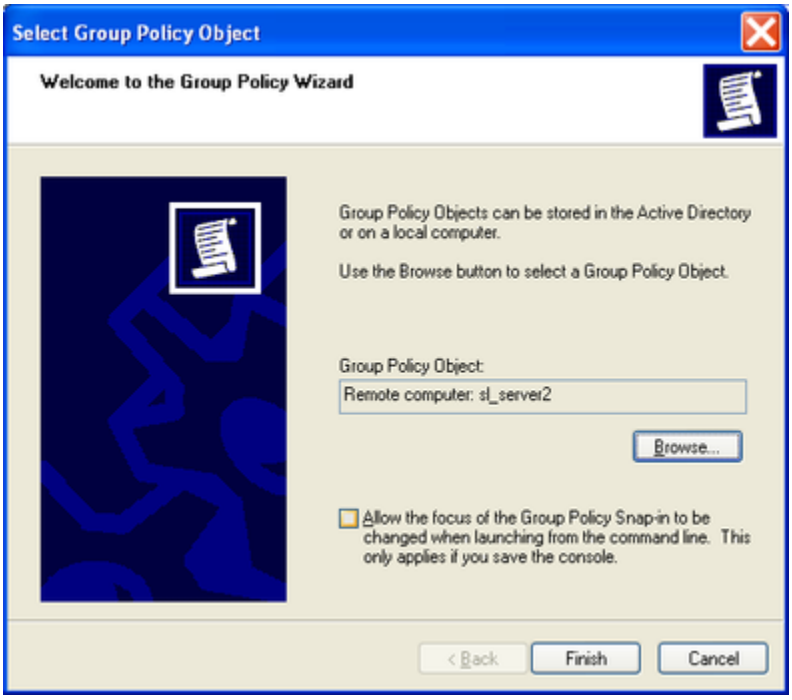
3. In the **Add/Remove snap-in** dialog box, click the **Standalone** tab, and then click **Add**.



4. Select **Group Policy** from the list, then click **Add**.



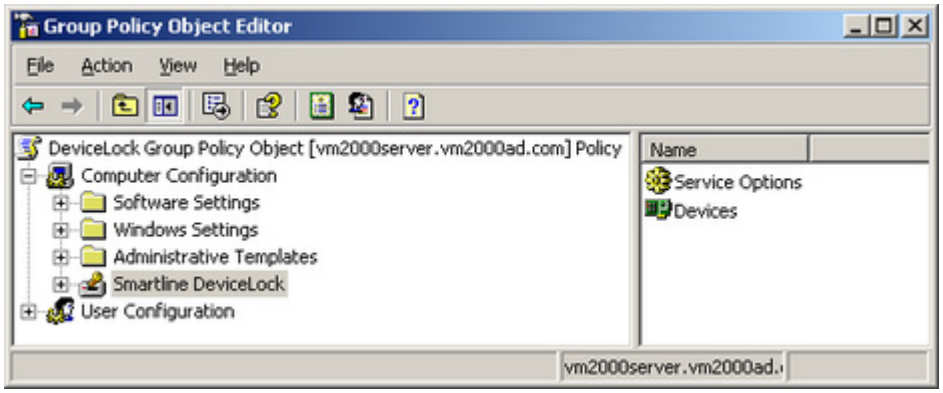
5. Select a Group Policy Object either from Active Directory or a local computer, and then click **Finish**.


Select Group Policy Object
Welcome to the Group Policy Wizard
Group Policy Objects can be stored in the Active Directory or on a local computer.
Use the Browse button to select a Group Policy Object.
Group Policy Object:
Remote computer: sl_server2
Browse...
Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.
< Back
Finish
Cancel

6. Click **Close** to close the **Add Standalone Snap-in** window.
7. Click **OK** to add the snap-in.
8. Expand the **Computer Configuration** container, and then select **DeviceLock**.

Using DeviceLock Group Policy Manager

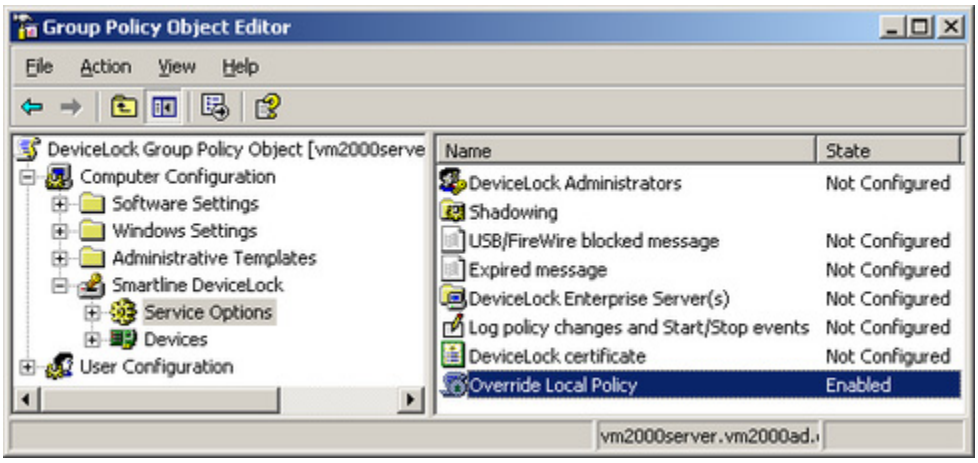
There is almost no difference between the procedure of managing DeviceLock Service via DeviceLock Management Console and via DeviceLock Group Policy Manager. For more information, see "Managing DeviceLock Service for Windows."



It is impossible to manage DeviceLock Enterprise Server and view audit and shadow logs using DeviceLock Group Policy Manager. For such operations you should use DeviceLock Management Console.

DeviceLock Service management via DeviceLock Group Policy Manager includes four additional features in comparison to DeviceLock Management Console:

1. **Override Local Policy** – If you want to disallow changing settings, permissions and audit rules for individual computers (without the GPO editor), enable **Override Local Policy** in **Service Options**. This enables the Group Policy mode for all the computers in GPO, so that the Local Policy mode cannot be enabled for these computers.



If the Override Local Policy parameter is enabled, it means that the Use Group Policy parameter in Service Options of DeviceLock Management Console and DeviceLock Enterprise Manager cannot be disabled.

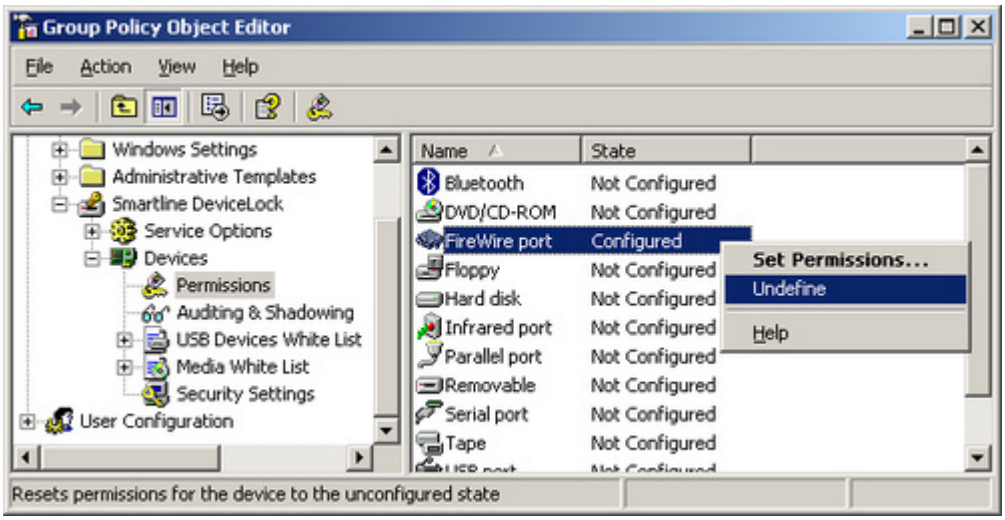
The following table shows how different settings of the **Use Group Policy** parameter and the **Override Local Policy** parameter affect the policy application mode:

POLICY APPLICATION MODE	USE GROUP POLICY	OVERRIDE LOCAL POLICY
Only Local Policy is applied.	Disabled	Disabled
Only Group Policy is applied.	Enabled	Enabled
Local Policy is applied until Active Directory replication occurs.	Enabled	Disabled

When setting the **Override Local Policy** parameter, consider the following:

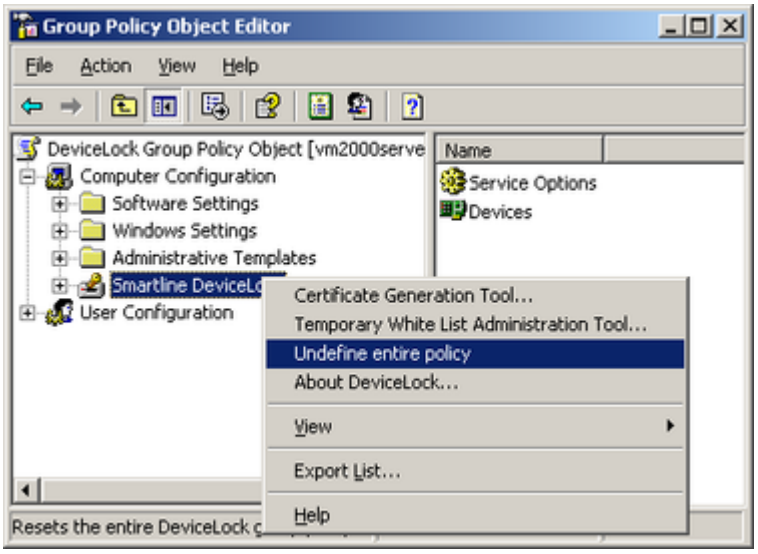
- Disabling the **Override Local Policy** parameter does not cancel Active Directory replication.
- If the **Override Local Policy** parameter is disabled, all DeviceLock Service settings that you set via DeviceLock Management Console and DeviceLock Enterprise Manager take effect immediately.

2. **Undefine** – You can reset any parameter to the unconfigured state. All undefined parameters are ignored in this GPO. For more information, see "Standard GPO Inheritance Rules."

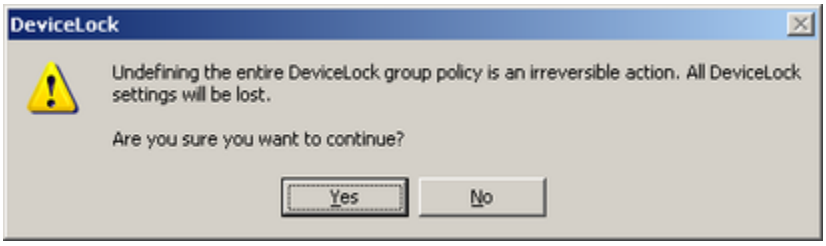


Use **Undefine** from the context menu of any parameter to reset this parameter to the unconfigured state. Also, for some parameters, you can use the intermediate state (gray) of the check box to make it unconfigured.

3. **Undefine entire policy** – You can reset all parameters to the unconfigured state in one click. Selecting this has the same effect as resetting each parameter one by one (see above).



Use **Undefine entire policy** from the context menu of **DeviceLock** to reset all parameters to the unconfigured state.


DeviceLock
Undefining the entire DeviceLock group policy is an irreversible action. All DeviceLock settings will be lost.
Are you sure you want to continue?
Yes
No

4. **Remove Offline** - You can remove any offline policy settings (permissions, audit, shadowing rules and alerts, white lists, etc.) for both devices and protocols in order to enforce regular ones in this GPO. To do so, right-click any policy setting, and then click **Remove Offline**.

Note: In order to manage DeviceLock Service settings via Group Policy, DeviceLock Service must be installed and started on all the computers belonging to the GPO. For more information about the service installation, see "Deploying DeviceLock Service."

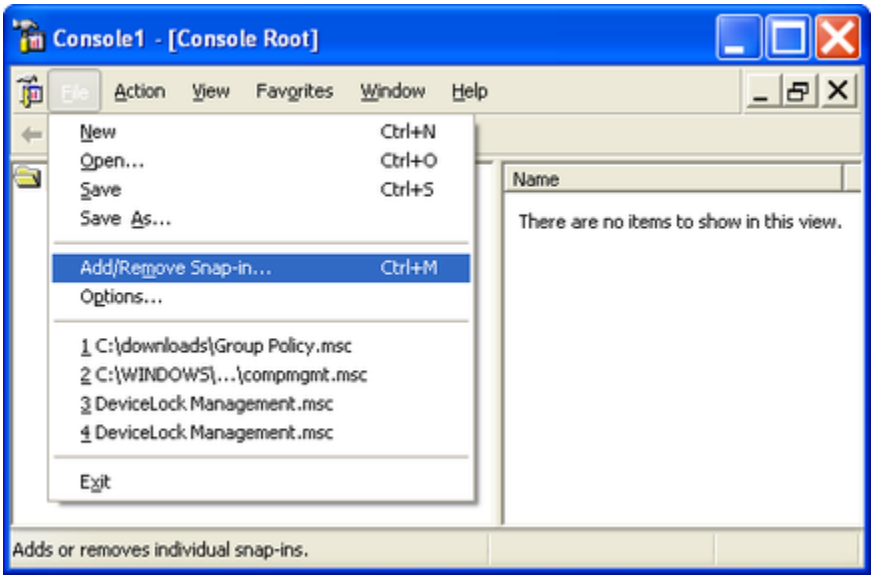
Also, do not forget that Group Policy is reapplied on a periodic basis (by default, every 90 minutes) so your changes do not take effect immediately. For more information, see "Applying Group Policy."

Using Resultant Set of Policy (RSoP)

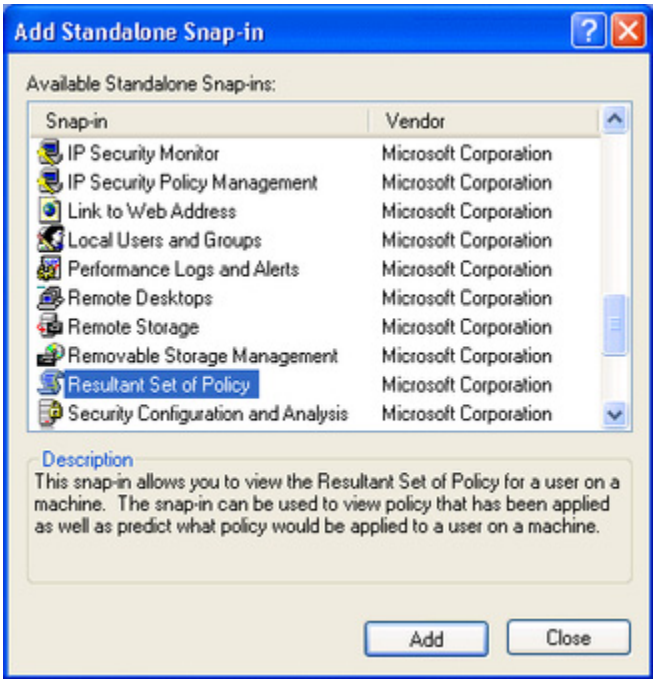
DeviceLock supports Resultant Set of Policy so you can use the standard Windows snap-in to view the DeviceLock policy currently being applied, as well as to predict what policy would be applied to a chosen computer.

To use RSoP, you should start MMC and add the Resultant Set of Policy snap-in manually:

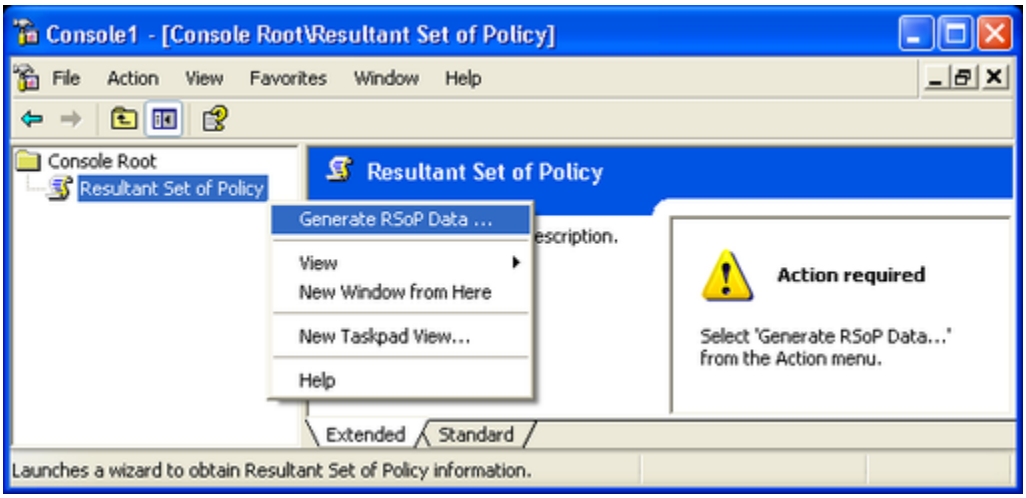
1. Run **mmc** from the command line or use the **Run** menu to execute this command.
2. On the **File** menu, click **Add/Remove snap-in**.



3. Click the **Standalone** tab, and then click **Add**.
4. Select **Resultant Set of Policy** from the list, then click **Add**.

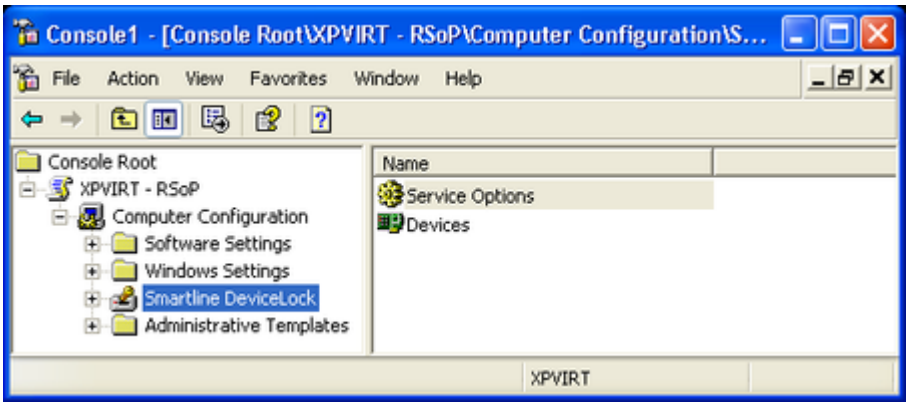


5. Click **Close** to close the **Add Standalone Snap-in** window and then click **OK** to add the snap-in.
6. In the console tree, select **Resultant Set of Policy**.



7. Click **Generate RSoP Data** on the context menu available by a right mouse click.
8. Go through the Resultant Set of Policy Wizard to obtain RSoP information from the selected computer.

9. Expand the **Computer Configuration** container, and then select **DeviceLock**.



Please note that using RSoP you cannot modify the policy – all parameters are in the read-only mode.

RSoP is very useful when you need to understand which particular GPO will be applied to the computer.

For more information on Resultant Set of Policy, please refer to the Microsoft's on-line article: http://technet.microsoft.com/en-us/library/cc775741%28WS.10%29.aspx.

Managing DeviceLock Service for Mac via Group Policy

DeviceLock Service for Mac can retrieve configuration settings from Active Directory via DeviceLock Enterprise Server. In order to enable DeviceLock Service for Mac to receive settings from group policies, perform the following steps:

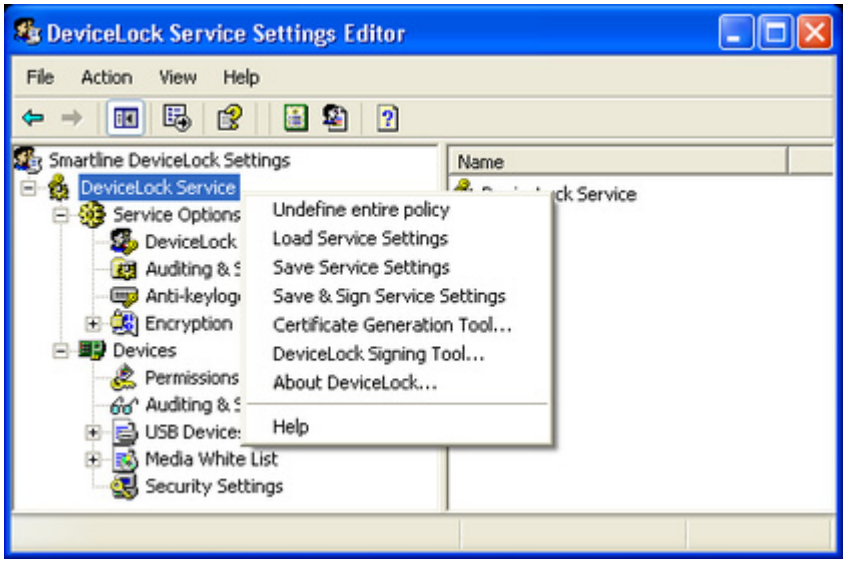
1. Register the Mac computer in the Windows domain.
2. Place the newly added computer into the required OU and configure policies according to your requirements.
3. Install DeviceLock Enterprise Server. No specific settings are required. Make sure that the computer hosting DeviceLock Enterprise Server has access to the domain controller with which the Mac computer is registered.
4. On the Mac computer, enter the address of DeviceLock Enterprise Server configured during the previous step.
5. Group policies will be propagated when any of the following conditions is reached:
   a) On reboot.
   b) Every hour.
   c) Forced update (by using the ***/Library/DeviceLockAgent/Utilities/DLAgentControl gpupdate*** command).
   d) When the **DeviceLock Enterprise Server(s)** parameter is changed in Service Options.

DeviceLock Service Settings Editor

Overview

DeviceLock Service Settings Editor is used for creating and modifying external XML files with settings, permissions, audit, shadowing rules and alerts for DeviceLock Service.

DeviceLock Service Settings Editor installs together with the other management consoles.



There is almost no difference between the procedures for defining policies via DeviceLock Management Console versus via DeviceLock Service Settings Editor. For more information, see "Managing DeviceLock Service for Windows."

In comparison to DeviceLock Management Console, in DeviceLock Service Settings Editor:

- You do not need to connect to any computer with DeviceLock Service. DeviceLock Service Settings Editor modifies and stores settings in external XML files and allows you to create/edit policies offline. It works similar to DeviceLock Group Policy Manager but instead of GPOs it uses XML files.
- You can reset any parameter (or all parameters at once) to the unconfigured state. All undefined parameters are ignored when the policy is applied to DeviceLock Service.
- You can remove any offline policy settings (permissions, audit, shadowing rules and alerts, white lists, etc.) for both devices and protocols in order to enforce regular ones in this policy file.

To create a new policy from scratch, just run DeviceLock Service Settings Editor and start making changes in its default (empty) policy.

If you want to modify an existing policy, you should load the XML file with that policy to DeviceLock Service Settings Editor using the **Load Service Settings** context menu command and then make desired changes.

If you create a new policy from scratch, you should use **Save Service Settings** from the context menu to save it in an XML file. Alternatively, you can use **Save & Sign Service Settings** from the context menu to save the policy to an external XML file and automatically sign it with the most recent DeviceLock Certificate (the private key). The **Save & Sign Service Settings** command is unavailable when the DeviceLock Signing Tool has no previously loaded private key.

Later files with policies created using DeviceLock Service Settings Editor can be loaded via DeviceLock Management Console and/or DeviceLock Group Policy Manager.

Also, files with policies can be sent to users whose computers are not online and thus out-of-reach via management consoles. To avoid unauthorized modification these files should be signed with the DeviceLock Certificate (the private key) using the DeviceLock Signing Tool. For more information, see "Service Settings."

If you modify an existing policy file, DeviceLock Service Settings Editor automatically saves your changes.

Note: Only settings that are explicitly defined in a policy file apply to client computers. All policy settings that have the **Not Configured** state are ignored by client computers.

DeviceLock Service Settings Editor is also used in the Set Service Settings plug-in of DeviceLock Enterprise Manager. This plug-in runs DeviceLock Service Settings Editor as an external application and opens it with the XML file selected in the plug-in's settings dialog box.

When you make any policy changes (change parameters, set permissions, define white lists, etc.) in the XML file passed to the editor by the plug-in, DeviceLock Service Settings Editor automatically saves them to this file. As soon as you finish modifying the policy just close DeviceLock Service Settings Editor and return to the plug-in's settings dialog box.

For more information, see "Set Service Settings."

DeviceLock Enterprise Manager

Overview

With DeviceLock Enterprise Manager, you can view and change security policies defined for device types and protocols; install, update and uninstall DeviceLock Service; and view audit and shadow logs for all the computers in a large network. We recommend using DeviceLock Enterprise Manager if you have a large network without Active Directory.

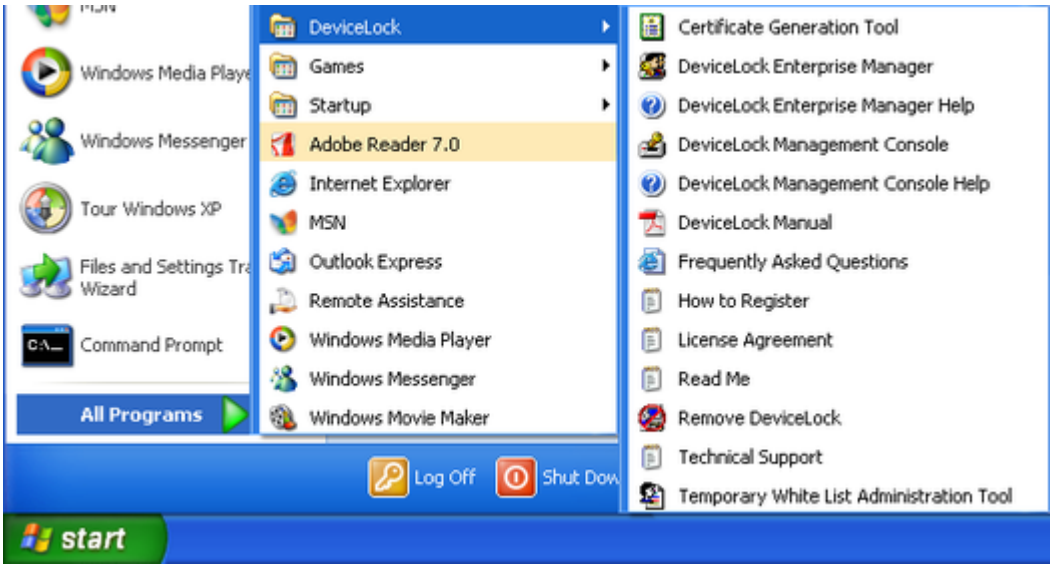
Based on a multi-threaded engine, using this console speeds up all activity for all the computers in the large network.

DeviceLock Enterprise Manager stores, compares and filters the data it receives from all the computers. Administrators can make "snapshots" of the systems for future comparison and notation of changes.

DeviceLock Enterprise Manager has a flexible plug-in based architecture that allows you to plug in necessary modules on demand. Each module (plug-in) performs a task and displays retrieved information in its own window.

For information on how to install DeviceLock Enterprise Manager, please read the Installing Management Consoles section of this manual.

To run DeviceLock Enterprise Manager, select the appropriate shortcut from the **Programs** menu available by clicking the Windows **Start** button.



Interface

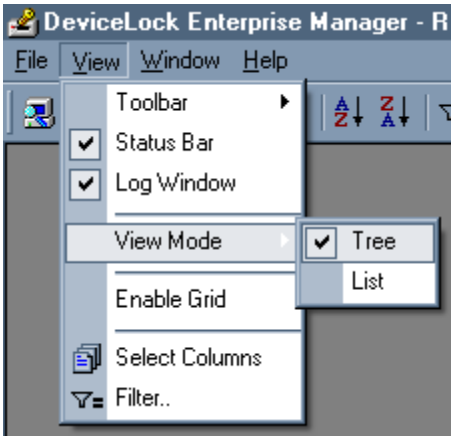
DeviceLock Enterprise Manager has a Multi Document Interface (MDI) structure, allowing you to keep each task in its own window.

The main window of DeviceLock Enterprise Manager can be resized. DeviceLock Enterprise Manager saves its size and position, and restores these at its next startup.

There is a menu at the top of the main window. Many functions are accessible through this menu.

To change the columns displayed in the plug-in's windows, click **Select Columns** on the **View** menu or click the appropriate button on the **Main** toolbar.

By default, DeviceLock Enterprise Manager displays information received from the plug-ins in the form of a tree. However, information can also be displayed as a plain list. To change the mode, point to **View Mode** on the **View** menu and click either **Tree** or **List**. Please note that View Mode must be set for each plug-in individually.



You can hide the status bar and/or the log window by deselecting appropriate items on the **View** menu.

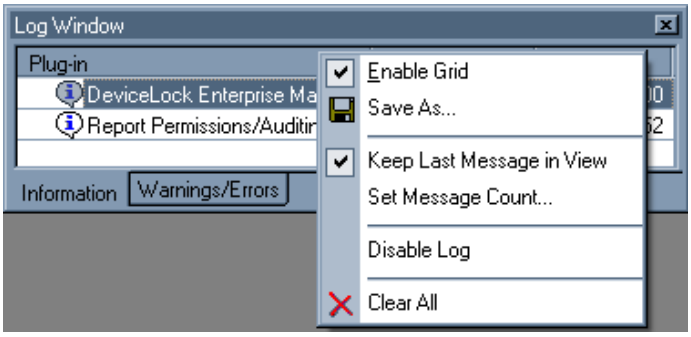
To enable the gridlines around items in the plug-in's window, click **Enable Grid** on the **View** menu. This mode sets for each plug-in individually.

To sort data in any plug-in's window, click the column heading you want to sort by. To reverse the sort order, click the column heading a second time.

If you need to sort the top-level tree's items (such as domains and computers), use appropriate buttons on the **Main** toolbar.

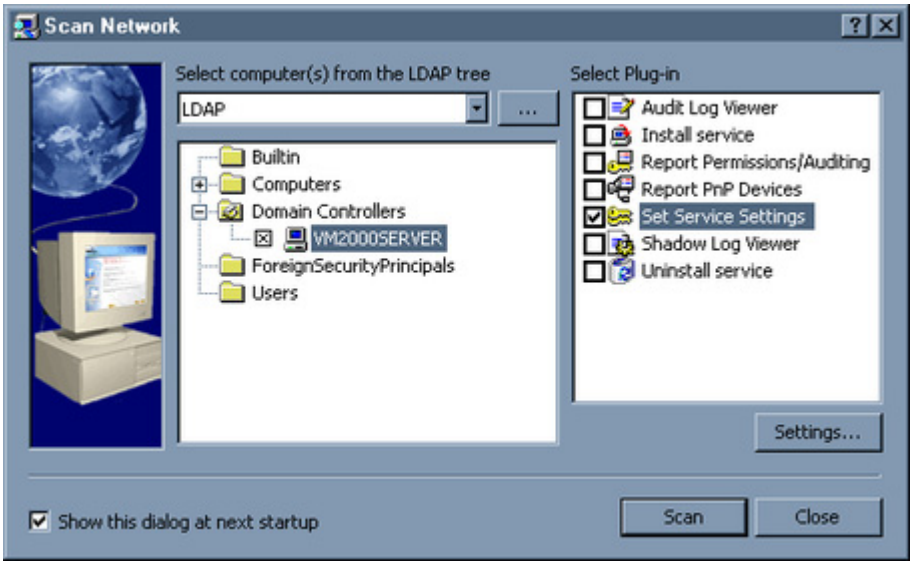
There is a log window at the bottom of the main window. The log window is used to display useful information about ongoing activity as well as diagnostic and error messages. There are two log lists: **Information** and **Warnings/Errors**.

You can click the right mouse button on the log window to open the useful context menu.



Scan Network Dialog Box

The **Scan Network** dialog box allows you to select computers on your network and the action (install or remove DeviceLock Service, set permissions, and so on) which should be performed for these computers.



To open the **Scan Network** dialog box, click **Scan Network** on the **File** menu or press the appropriate button on the **Main** toolbar. If the **Show this dialog at next startup** check box is selected, the **Scan Network** dialog box will open automatically each time DeviceLock Enterprise Manager is started.

There are three simple steps, which enable you to manage DeviceLock Services across the network.

Selecting Computers

The first step is to select the computers to be processed.

You can use the context menu, available by right clicking, to select/deselect necessary items (computers types, domains, or computers).

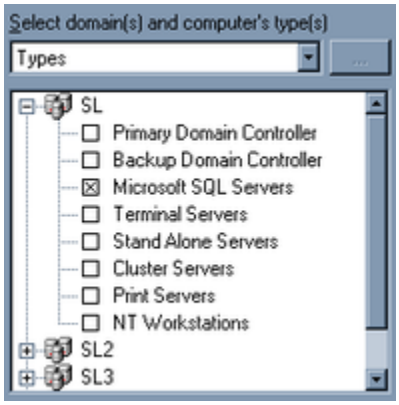
DeviceLock Enterprise Manager provides several flexible ways to select network computers.

- Network computers can be selected by their types.
  Each type represents all of the computers belonging to the category:
  - **Primary Domain Controller** – a primary domain controller.
  - **Backup Domain Controller** – a backup domain controller.
  - **Microsoft SQL Servers** – any server running with Microsoft SQL Server.
  - **Terminal Servers** – any server where Terminal Services are running.
  - **Stand Alone Servers** – any server that is not a domain controller.

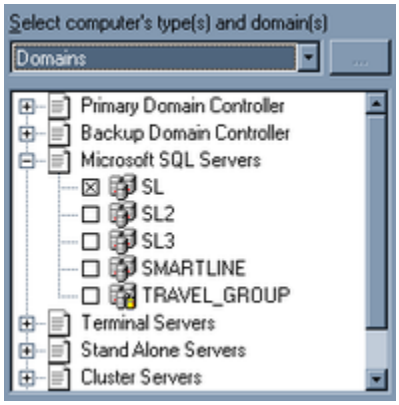
- **Cluster Servers** – server clusters available in the domain.
- **Print Servers** – any computer that is sharing the print queue.
- **NT Workstations** – any Windows NT/2000/XP/Vista/7/8 and Windows Server 2003/2008/2012 computer.

There are two ways to choose the type of computers:

1. **Types** – you select the network domain and then select types of computers which must be processed in this domain.



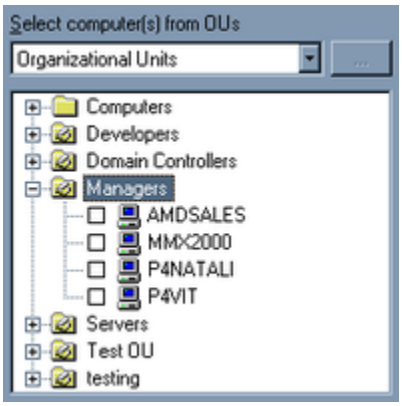
2. **Domains** – you select the type of computer and then select network domains where computers of the selected type must be processed.



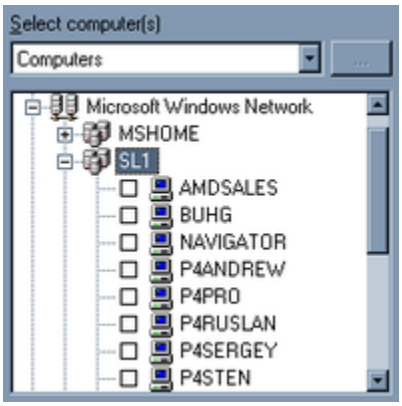
- Network computers can also be selected by their names.

  There are several ways to choose computers by name:

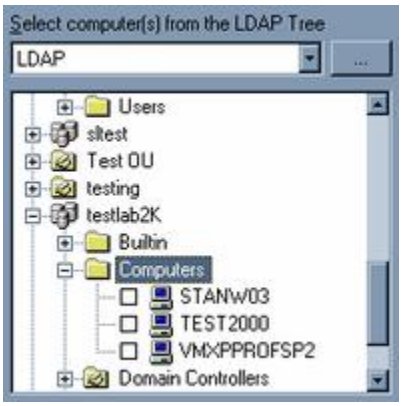
  1. **Organizational Units** – you browse Active Directory organizational units (OUs) and select computers, which must be processed.



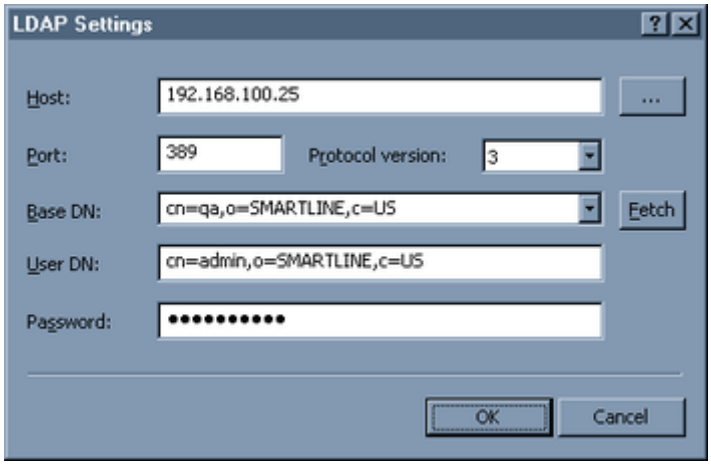
2. **Computers** – you browse the network tree and select computers.



3. **LDAP** – you browse the LDAP (Lightweight Directory Access Protocol) tree and select computers from the directory.



To configure a connection to the LDAP server, click the **...** button.



Host – the name or the IP address of the LDAP server to connect to.

Port – the TCP port on which the LDAP server accepts connections. The default port is 389.

Protocol version – the LDAP protocol version. Some servers are not fully compatible with the LDAP v.3 protocol and LDAP requests require certain adjustments for correct communication with such servers. Selecting **Version 2** makes sure that the server requests are adjusted according to the LDAP v.2 protocol requirements.

Base DN – the starting point for you to browse the directory tree. You must use the LDAP string representation for distinguished names (for example, cn=qa,o=SMARTLINE,c=US). Leave the **Base DN** box blank to start browsing from the root.

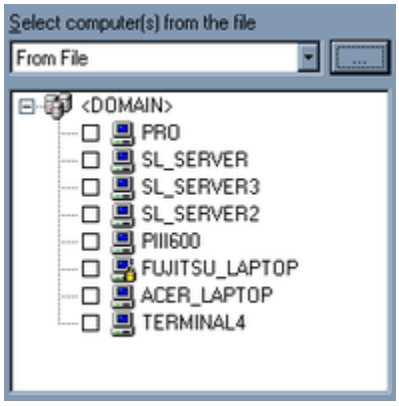
By clicking the **Fetch** button, you can get all the published naming contexts.

User DN – the distinguished name (DN) of the directory user that allows connection to the directory. You must use the LDAP string representation for distinguished names (for example, cn=admin,o=SMARTLINE,c=US).

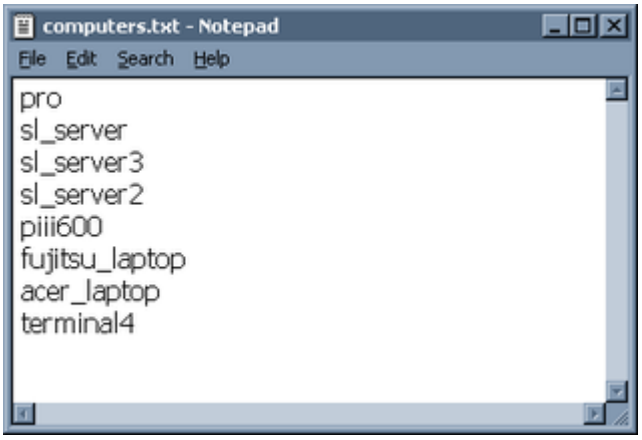
Password – the user's password.

4. **From File** – you load a predefined list of computers from the external text file and then select the computers.

   To open an external file, click the **...** button.

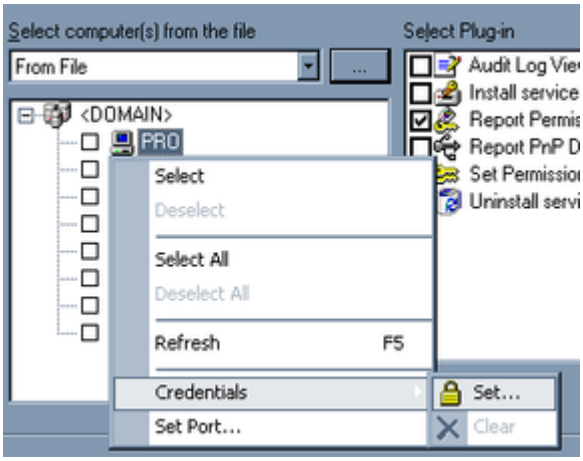


A text file must contain each computer's name or IP address on separate lines and can be either Unicode or non-Unicode. A brief example of such a file follows:



Supplying Credentials

If you need to supply alternative credentials for the target computer(s), select the computer or network domain from the tree and point to **Credentials** on the context menu.

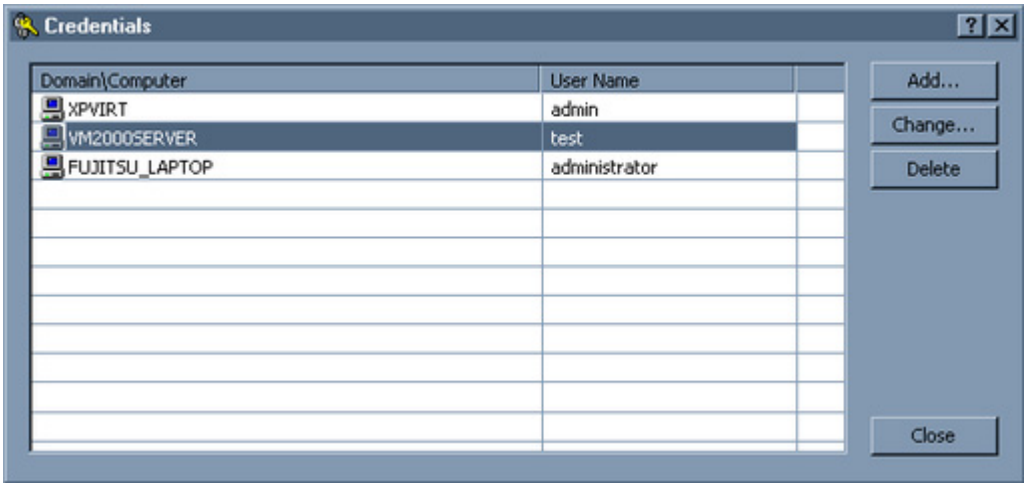


You may assign credentials to individual computers and/or to network domains. To add credentials, click **Set**. To delete alternative credentials, click **Clear**.

Credentials consist of a user name and password pair used to authenticate the computers processed. By default, DeviceLock Enterprise Manager uses your currently logged on credentials to automatically log in and process the target computer(s). If the current logged-in user credentials do not have administrative rights on all of the target computers, you need to enter alternate credentials. DeviceLock Enterprise Manager will use these alternate credentials to automatically login to the target computers.

In all cases, credentials are stored with encryption techniques and are not available to anyone except the user with administrative privileges.

Credentials can also be supplied via the **Credentials** dialog box. To open the **Credentials** dialog box, click **Credentials** on the **File** menu.

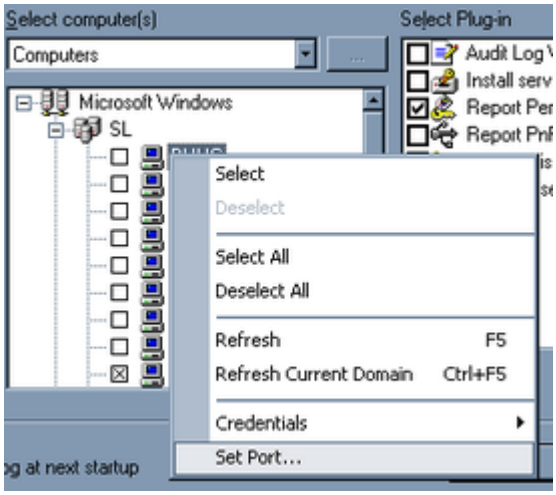


Click **Add** to add new credentials. To change existing credentials, select the record in the list and click **Change**.

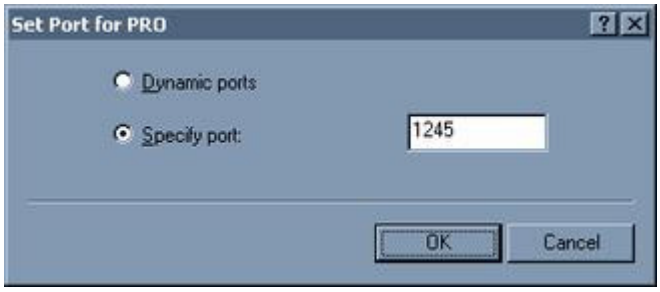
To delete credentials, select the record in the list and click **Delete**. Using CTRL and/or SHIFT you can select and remove several records simultaneously.

Setting Port

You can instruct DeviceLock Enterprise Manager to use a fixed port, making it easier to configure a firewall. To do so, use **Set Port** from the context menu.



By default, DeviceLock Enterprise Manager uses dynamic ports for RPC communication with DeviceLock Service. However, if DeviceLock Service is configured to accept connections on a fixed port, select the **Specify port** option.



To use the dynamic ports binding, click **Dynamic ports**.

DeviceLock Service can be configured to use either a fixed port or dynamic ports during the installation process. For more information on this, see "Unattended Installation" and "Remote Installation via DeviceLock Enterprise Manager."

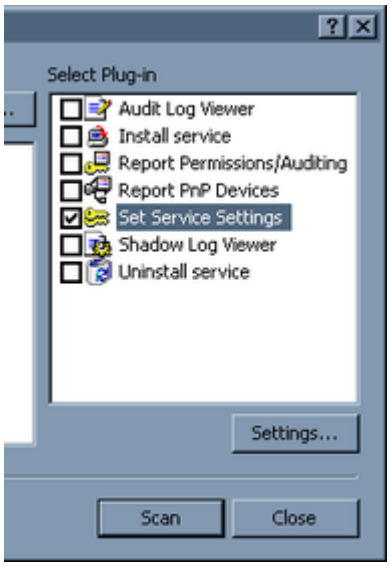
If you need to change the port configuration when DeviceLock Service is already installed, use the Install service plug-in.

For information on which ports are required for which actions, see "Plug-ins."

Selecting Plug-ins

The second step is to select a plug-in to process the network computers selected on the first step.

To select/deselect plug-ins, you can use the context menu available with a right mouse click.



To define parameters for the selected plug-in, use the **Settings** button below the plug-ins list. If the plug-in does not have additional parameters, this button is unavailable.

Tasks are passed to the plug-in by DeviceLock Enterprise Manager.

The plug-in performs the task and returns the information to DeviceLock Enterprise Manager. Upon receipt of a plug-in's information, DeviceLock Enterprise Manager displays it in a separate window.

Starting a Scan

Once you have selected computers and the appropriate plug-in, the final step is starting the scan process. Click **Scan** to initiate the process.

Right after the scan process is initiated, you can start to explore the information that is already received from the plug-in.

Because the scan process runs in a separate thread, you do not need to wait until all computers are finished being scanned. You can also perform other tasks in the DeviceLock Enterprise Manager interface.

There are only a few things which you cannot do while the scan is running – you cannot close DeviceLock Enterprise Manager and you cannot run another scan process.

If, for some reason, you wish to abort the active scan process, you can click **Stop Scan** on the **File** menu or press the appropriate button on the **Main** toolbar. The scan process will be aborted as soon as a plug-in returns control to DeviceLock Enterprise Manager.

Plug-ins

DeviceLock Enterprise Manager has a flexible plug-in based architecture that allows you to plug in the necessary module on demand. DeviceLock Enterprise Manager loads the plug-ins on startup from the ***Plugins*** subdirectory, which is located in the main DeviceLock Enterprise Manager directory.

DeviceLock Enterprise Manager ships with standard plug-ins that require some network ports to be opened on remote computers, as described in the table below:

REQUIRED PORTS	PLUG-INS AFFECTED
TCP 139 or TCP 445 **UDP 137** – this port must be opened only when a connection is established by the computer name. If an IP address is used, this port is not required.	Audit Log Viewer, Report PnP Devices
TCP 139 or TCP 445 **UDP 137** – this port must be opened only when a connection is established by the computer name. If an IP address is used, this port is not required.	Install Service, Uninstall Service
TCP 139 or TCP 445 **TCP 135** – this port is required only when the **Dynamic ports** connection is used. **TCP <all ports above 1024>** – these ports are required only when the **Dynamic ports** connection is used. **TCP <custom port>** – this port is required only when the **Fixed port** connection is used. **UDP 137** – this port must be opened only when a connection is established by computer name. If an IP address is used, this port is not required.	Report Permissions/Auditing, Set Service Settings, Shadow Log Viewer

For information on how to use either the **Dynamic ports** or **Fixed port** connection in DeviceLock Enterprise Manager, see "Setting Port."

When a plug-in is connected to a remote computer it may receive some of these error messages:

- **The product version on the client and server machines does not match (7049)** – you are trying to connect to a computer where an old version of DeviceLock Service is installed. You should upgrade DeviceLock Service first using the Install Service plug-in.
- **The network path was not found (53)** – you are trying to connect to a computer that either does not exist (the wrong name or IP address) or is not accessible. Make sure that the computer name you have specified is correct. Try to access this computer with Windows Explorer and connect to it using any standard Windows administrative tool (such as Computer Management, Services and so on).

This error also occurs when the standard Windows Server service is not running on the remote computer. Check the Server service status and start it if it is stopped.

More connection errors are described in the Possible Connection Errors section of this manual.

Audit Log Viewer

The Audit Log Viewer plug-in retrieves DeviceLock's audit log from the computer's local Windows event logging subsystem.

To define a maximum log size and what Windows should do if the audit log becomes full, use **Audit Log Settings** from the context menu.

To clear all events from the audit log, select **Clear Audit Log** from the context menu.

For more information, see "Audit Log Viewer (Service)."

Install Service

The Install Service plug-in installs or updates DeviceLock Service on computers.

Note: Only the built-in administrator account can be used to perform a remote installation of DeviceLock Service on computers running Windows Vista or a later version of Windows. In a Windows Active Directory environment, only members of the Domain Admins group can perform a remote installation of DeviceLock Service. Administrator privileges are required to connect to DeviceLock Service via DeviceLock Management Console. For more information, refer to Microsoft's article.

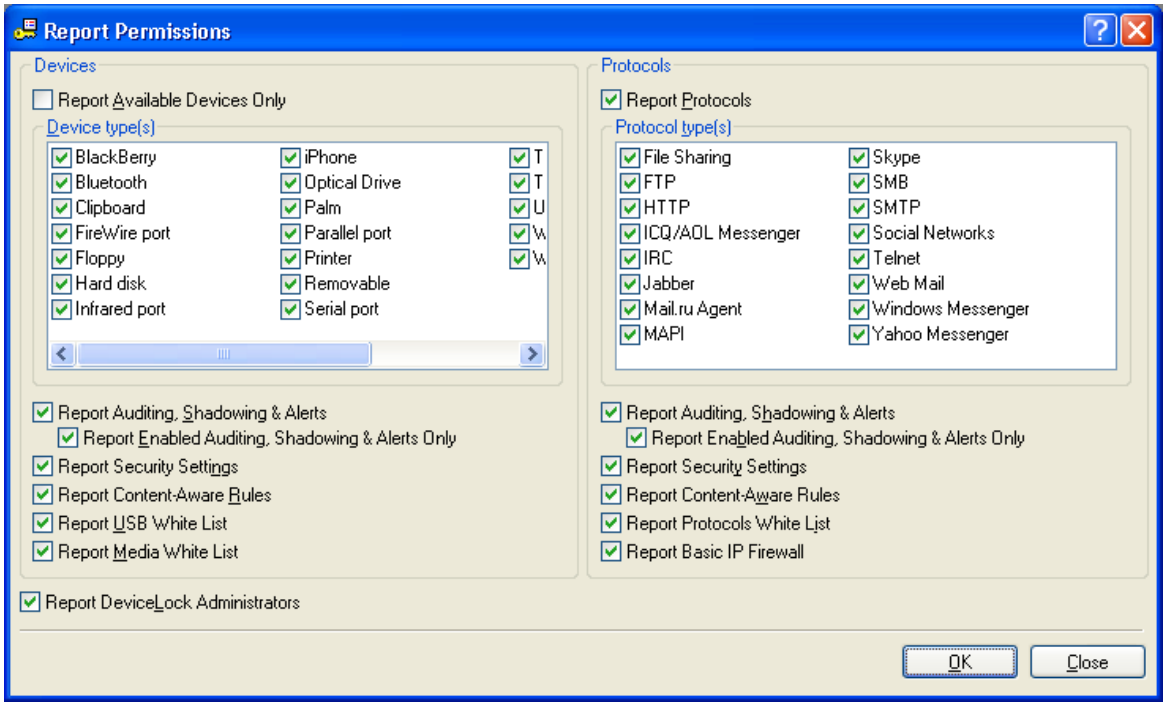
Before you can use this plug-in, you should specify the directory that contains all of the files needed for installation (such as DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe, and InstMsiW.exe). You can do this by clicking the **Settings** button below the plug-ins list in the **Scan Network** dialog box (see "Selecting Plug-ins").

For more information, see "Remote Installation via DeviceLock Enterprise Manager."

Report Permissions/Auditing

The Report Permissions/Auditing plug-in generates a report that allows you to view and change security policies defined for device types and protocols across the network.

Before you can use this plug-in, you should select the information you want to include in the report. You can do this by clicking the **Settings** button below the plug-ins list in the **Scan Network** dialog box (see "Selecting Plug-ins").



In the **Report Permissions** dialog box, specify the information that you want to include in your report.

To receive information on the security policies defined for device types, under **Devices**, use the following options:

- **Report Auditing, Shadowing & Alerts** – select this check box to report audit, shadowing rules and alerts that have been set. Also when this check box is selected, you receive information about whether the **Log Policy changes and Start/Stop events** parameter is enabled in Service Options.
- **Report Enabled Auditing, Shadowing & Alerts Only** – select this check box to exclude devices for which audit, shadowing rules and alerts are disabled from the report.

  This option is available only if the Report Auditing, Shadowing & Alerts check box is selected.
- **Report Security Settings** – select this check box to report what parameters are disabled via Security Settings.
- **Report Content-Aware Rules** - select this check box to report Content-Aware Rules that have been set (see "Content-Aware Rules for Devices").
- **Report USB White List** – select this check box to include information about white listed devices (see "USB Devices White List").
- **Report Media White List** – select this check box to include information about white listed media (see "Media White List").

- **Report DeviceLock Administrators** – select this check box to report accounts that can manage DeviceLock Service or view its settings and logs.

To receive information on the security policies defined for protocols, under **Protocols**, use the following options:

- **Report Protocols** – select this check box to report security policies for protocols. Otherwise, information on all protocol-based policies will be excluded from the report.
  If the Report Protocols check box is cleared, the Report Auditing, Shadowing & Alerts option and the Report Enabled Auditing, Shadowing & Alerts Only option are unavailable.
- **Report Auditing, Shadowing & Alerts** – select this check box to report audit, shadowing rules and alerts that have been set for protocols.
- **Report Enabled Auditing, Shadowing & Alerts Only** – select this check box to exclude protocols for which audit, shadowing rules and alerts are disabled from the report.
  This option is available only if the Report Auditing, Shadowing & Alerts check box is selected.
- **Report Security Settings** – select this check box to report what parameters are defined via Security Settings.
- **Report Content-Aware Rules** - select this check box to report Content-Aware Rules that have been set for protocols (see "Content-Aware Rules for Protocols").
- **Report Protocols White List** – select this check box to include information about white listed protocols (see "Managing Protocols White List").
- **Report Basic IP Firewall** – select this check box to report Basic IP Firewall rules that have been set (see "Managing Basic IP Firewall").

This report always includes information about an installed DeviceLock Certificate. Also, it always shows when the **Use Group Policy** parameter is enabled in Service Options.

Report PnP Devices

The Report PnP Devices plug-in generates a report displaying the USB, FireWire and PCMCIA devices currently connected to computers on the network and those that were connected.

Note: In order to retrieve PnP devices from Windows Vista/7 and Windows Server 2008 computers, you should allow remote access to the PnP interface on those computers. You can do it via modifying the policy as described in this article: support.microsoft.com/kb/947040.

This plug-in does not work for computers running Windows 8 and later systems.

The columns are defined as follows:

- **Description** – the description of the device provided by its vendor.

- **Device Information** – the additional information about the device provided by its vendor.
- **Connected to** – the interface where the device is connected (USB, FireWire or PCMCIA).
- **Class** – the class of the device provided by Windows.
- **Class description** – the description of the device's class provided by Windows.
- **Present** – indicates whether the device is currently connected or not (**Yes** or **No**).
- **DeviceID** – the unique identification string of the device provided by its vendor.
- **Driver** – the name of the driver that is controlling this device.

You can add reported USB devices to the USB Devices Database using the context menu available via a right mouse click.

Before you can use this plug-in, you should select the information you want to include in reports. You can do this by clicking the **Settings** button below the plug-ins list in the **Scan Network** dialog box (see "Selecting Plug-ins").

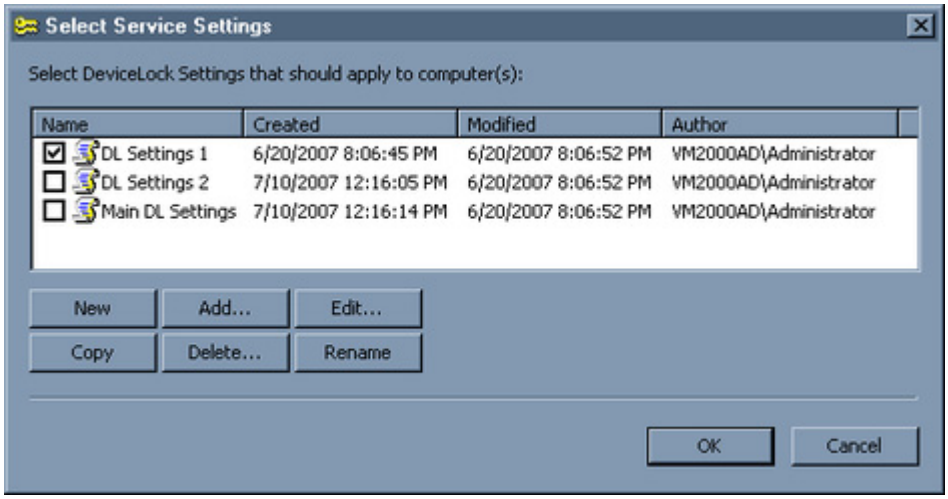
- **Report Connected Devices Only** – select this check box to report only those devices that are currently connected to the computer. Otherwise, you will see all devices that were ever connected to the computer.
- **Report FireWire Devices** – select this check box to report devices that are plugging into the FireWire port.
- **Report PCMCIA Devices** – select this check box to report devices that are plugging into the PCMCIA slot.
- **Report USB Devices** – select this check box to report devices that are plugging into the USB port.

Set Service Settings

The Set Service Setting plug-in reads the policy (settings, permissions, audit, shadowing rules and alerts) from the external XML file and deploys it to DeviceLock Services across the network.

Note: Only settings that are explicitly defined in a policy file apply to client computers. All policy settings that have the **Not Configured** state are ignored by client computers.

Before you can use this plug-in, you should define settings, permissions and/or audit rules that you want to deploy. You can do this by clicking the **Settings** button below the plug-ins list in the **Scan Network** dialog box (see "Selecting Plug-ins").



First of all you have to prepare the policy you want to deploy.

If there are no files in the list, then you can either create an empty file by clicking the **New** button or add an existing file by clicking the **Add** button.

Then select the file in the list and click **Edit** to open DeviceLock Service Settings Editor. DeviceLock Service Settings Editor is used for creating and modifying external XML files with settings, permissions, audit, shadowing rules and alerts for DeviceLock Service. For more information, see "DeviceLock Service Settings Editor."

When finished modifying the policy, select its file by selecting the check box next to the file's name in the list. Then click **OK** to close the configuration dialog box.

Shadow Log Viewer

The Shadow Log Viewer plug-in retrieves the shadow log from DeviceLock Service.

Use the context menu available by a right mouse click to access all this plug-in's functions.

For more information, see "Shadow Log Viewer (Service)."

Uninstall Service

The Uninstall Service plug-in removes DeviceLock Service and all its settings and components from computers.

If the user under which DeviceLock Enterprise Manager is connecting to the computer does not have full administrative access to DeviceLock Service, the plug-in will not be able to remove the service.

Likewise, an error occurs when the user does not have local administrative privileges on the computer where DeviceLock Service is running.

Open / Save / Export

DeviceLock Enterprise Manager can store all information received from plug-ins.

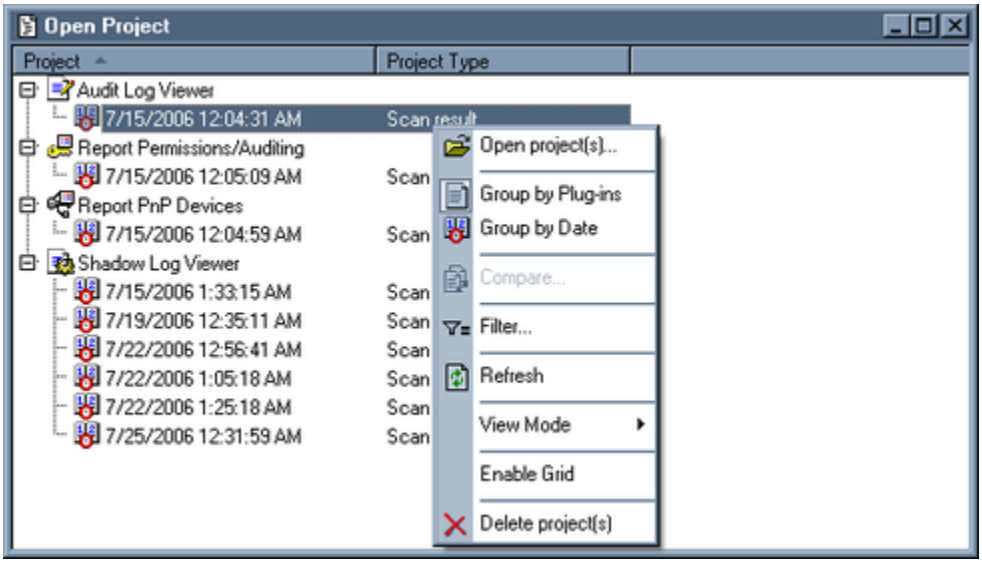
The data is saved to external files and is ready for loading into DeviceLock Enterprise Manager when requested.

There are three ways to save and load data:

1. The handiest method to store received information is to save it as a project. When you are saving data as a project, DeviceLock Enterprise Manager saves each active plug-in's window to a separate file of its own format and places this file in the ***Project*** subdirectory.

   The names of the project's files are auto-generated and depend on the plug-in's names and the date and time when the scan was started.

   To save the data as a project, you can select **Save Project** from the **File** menu or press the appropriate button on the **Main** toolbar.



   To load previously saved projects, select **Open Project** from the **File** menu.

   The **Open Project** window has its own toolbar and context menu available by a right mouse click.

   You can group saved projects by the date when they were scanned and by the type of information they contain. Select **Group by Plug-ins** or **Group by Date** from the context menu or press appropriate buttons on the **Project** toolbar.

To open a saved project, select it from the list and press the **Open Project** button on the **Project** toolbar. Using CTRL and/or SHIFT, you can select and open several projects simultaneously.

2. Another way to save received information in the format of DeviceLock Enterprise Manager is select **Save As** from the **File** menu. This enables you to save a file of the ANM type to any place on your hard disk or any other media with any name you choose.

   To load previously saved files, you can select **Open** from the **File** menu or press the appropriate button on the **Main** toolbar. You will need to specify a file you wish to open. You can load files of the ANM type only.

3. If you need to pass received information to a third-party application, you can export it into an external file and then import it to this application. To export data into the external file, select **Save As** from the **File** menu and then select the file's type from the **Save as type** box. DeviceLock Enterprise Manager supports the export into MS Excel (if it is installed on the local computer) and two formats of text files – Tab Delimited (TXT) and Comma Delimited (CSV).

   If you export information into an external file, you will not be able to load it back to DeviceLock Enterprise Manager because DeviceLock Enterprise Manager can open and load only files of its own format. However, the ability to export into an external file is useful when you wish to exchange data between DeviceLock Enterprise Manager and other applications.

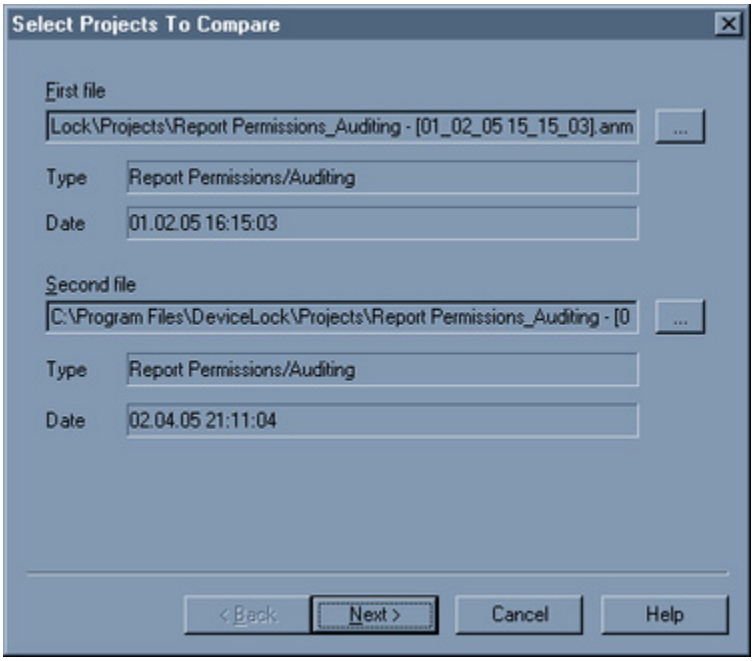
Comparing Data

DeviceLock Enterprise Manager allows you to track changes on network computers by comparing two previously saved projects. Tracking changes is important when managing a wide range of computers on one network.

DeviceLock Enterprise Manager provides a very useful and intuitive Wizard to compare two ANM files. To open this Wizard, select **Compare** from the **File** menu.

There are three simple steps, which enable you to compare two files using the Compare Wizard:

1. The first step is to select the files you want to compare.

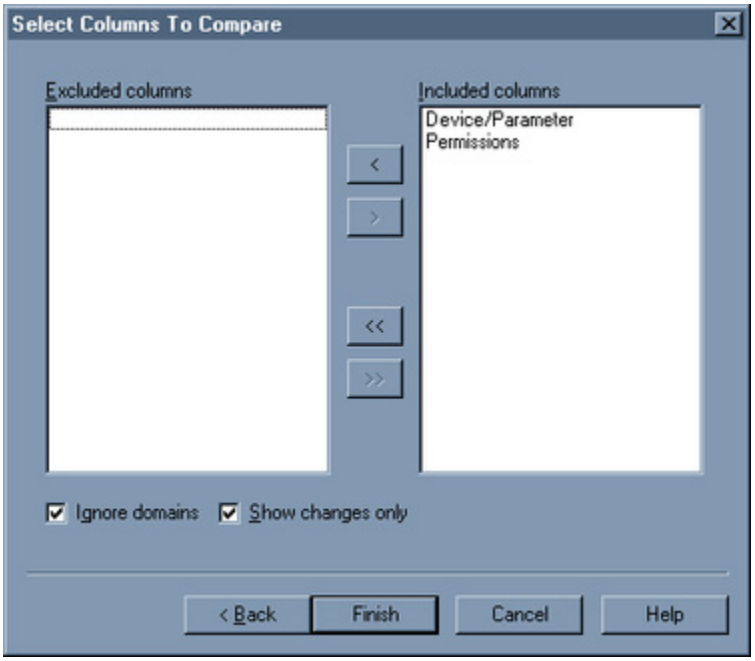


Select the first file and then select the second file by using the ellipsis (**...**) buttons.

Please note that you can compare files of the same type only. For example, you cannot compare information received from the Report Permissions/Auditing plug-in with information from the Report PnP Devices plug-in.

When you have selected two files, press the **Next** button to go to the Wizard's next page.

2. The second step is to select the columns you wish to include in the compare process.



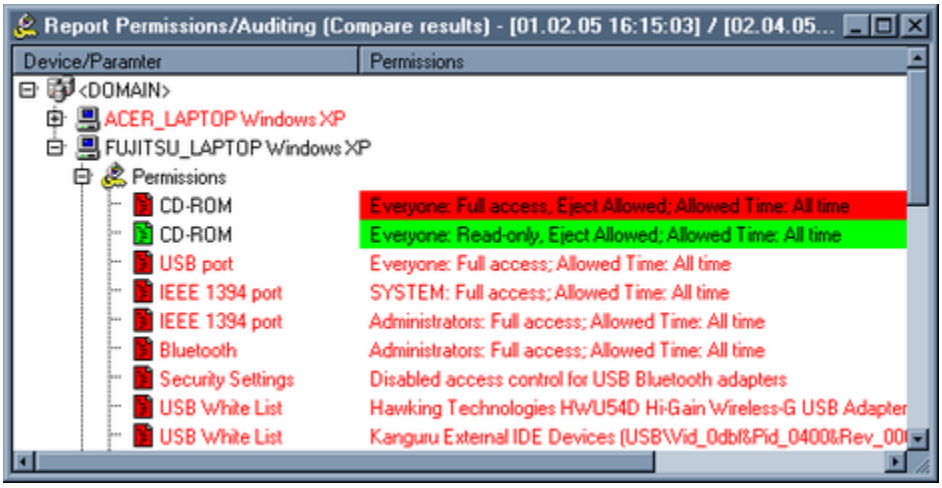
DeviceLock Enterprise Manager compares only those columns, which you have selected. If you need to exclude one column from the compare process, you have to move it from the **Included columns** list to the **Excluded columns** list. Excluded columns will be visible in the compare result, but the values they contain are ignored and do not affect the compare result.

By default, the compare result contains only records, which are different in the two files being compared. If you would like to see all of the records (even unchanged records), you can clear the **Show changes only** check box.

To include names of the network domains in the compare process, you can clear the **Ignore domains** check box. When the **Ignore domains** check box is selected, DeviceLock Enterprise Manager ignores domains and only compares computers and the information those computers contain.

3. The third and final step is to start the compare process. Press the **Finish** button to compare two selected files with each other.

   DeviceLock Enterprise Manager displays the compare result in a separate window in the form of a tree exactly as it displays information received from a plug-in.


Report Permissions/Auditing (Compare results) - [01.02.05 16:15:03] / [02.04.05...
Device/Paramter
Permissions
<DOMAIN>
ACER_LAPTOP Windows XP
FUJITSU_LAPTOP Windows XP
Permissions
CD-ROM
Everyone: Full access, Eject Allowed; Allowed Time: All time
CD-ROM
Everyone: Read-only, Eject Allowed; Allowed Time: All time
USB port
Everyone: Full access; Allowed Time: All time
IEEE 1394 port
SYSTEM: Full access; Allowed Time: All time
IEEE 1394 port
Administrators: Full access; Allowed Time: All time
Bluetooth
Administrators: Full access; Allowed Time: All time
Security Settings
Disabled access control for USB Bluetooth adapters
USB White List
Hawking Technologies HWU54D Hi-Gain Wireless-G USB Adapter
USB White List
Kanguru External IDE Devices (USB\Vid_0dbf&Pid_0400&Rev_00

The comparison is very simple and effective:

1. If the **Ignore domains** check box is cleared, the program enumerates network domains in the two selected files and tries to find each domain in both the older file and the recent file.

   If the domain exists in the older file but does not exist in the recent file, DeviceLock Enterprise Manager inserts the missing domain (along with all the computers contained in that domain as well as the information in those computers) into the comparison result and then writes all those records in red.

   If the domain does not exist in the older file but exists in the recent file, DeviceLock Enterprise Manager inserts the missing domain (along with all the computers contained in that domain as well as the information in those computers) into the comparison result and then writes all those records in green.

   If the domain exists in both files, DeviceLock Enterprise Manager enumerates all the computers the domain contains (see below).

2. If the **Ignore domains** check box is selected, DeviceLock Enterprise Manager ignores domains and enumerates all the computers in the two selected files and tries to find each computer in both older and recent files.

   If the computer exists in the older file but does not exist in the recent file, DeviceLock Enterprise Manager inserts the missing computer with all information it contains into the compare result and writes all these records in red.

   If the computer does not exist in the older file but exists in the recent file, DeviceLock Enterprise Manager inserts the missing computer with all information it contains into the compare result and writes all these records in green.

   If the computer exists in both files, DeviceLock Enterprise Manager enumerates all the information it contains (see below).

3. DeviceLock Enterprise Manager enumerates all information for a computer and tries to find each record in both the older and the recent file.

   If the record exists in the older file but does not exist in the recent file, DeviceLock Enterprise Manager inserts the missing record into the compare result and writes it in red.

   If the record does not exist in the older file but exists in the recent file, DeviceLock Enterprise Manager inserts the missing record into the compare result and writes it in green.

   If the record exists in both files, DeviceLock Enterprise Manager starts comparing each included column for this record:

   - If the column's values for the older and the recent files are different, DeviceLock Enterprise Manager inserts both records in the compare result. The record from the recent file comes right after the record from the older one.

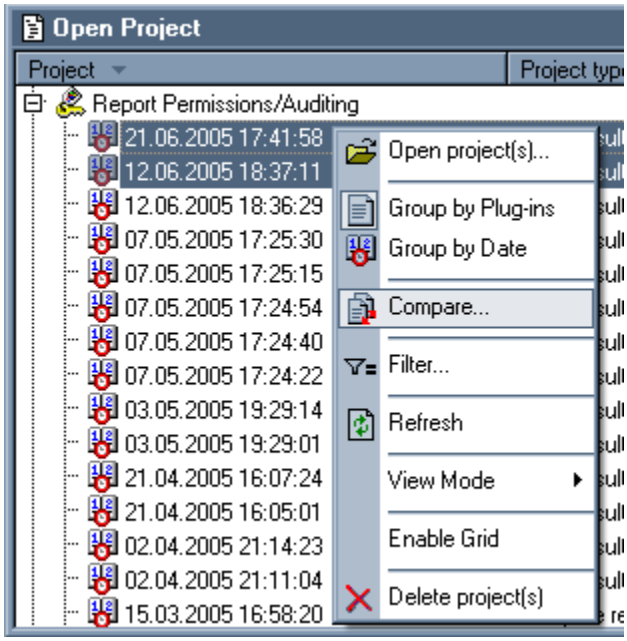
     The column that belongs to an older record is highlighted in red. The column that belongs to a recent record is highlighted in green. All excluded columns and columns with equal values are not highlighted and are written in the default color.

   - If all of a record's columns for both files contain equal values, DeviceLock Enterprise Manager either skips this record (the **Show changes only** check box is selected) or inserts this record into the compare result and writes it in the default color (the **Show changes only** check box is cleared).

If you wish to compare two files, which were saved as projects, it is a good idea to use the special feature of the **Open Project** window.

Select **Open Project** from the **File** menu, select two projects you would like to compare (use CTRL and/or SHIFT to select two projects simultaneously) and then select **Compare** from the context menu or press the appropriate button on the **Project** toolbar.

Please note that you may select only two projects and both projects must be of the same type.



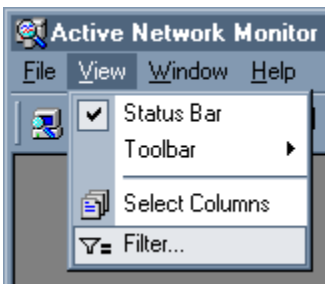
DeviceLock Enterprise Manager provides two buttons on the **Compare** toolbar, which help you to easily navigate through the compare result. Press the **<** button to select the previous record in the compare result that contains changes. Press the **>** button to select the next record in the compare result that contains changes.

You can also save the compare result to an external ANM file or export it into MS Excel or the text file (TXT and CSV). Select **Save As** from the **File** menu or press the appropriate button on the **Main** toolbar to save or export the compare result.

As with any other DeviceLock Enterprise Manager file, the saved compare result can be opened and loaded to DeviceLock Enterprise Manager. To load the previously saved compare result, you can select **Open** from the **File** menu or press the appropriate button on the **Main** Toolbar. You will need to specify a file you want to open. You can load files of ANM type only.

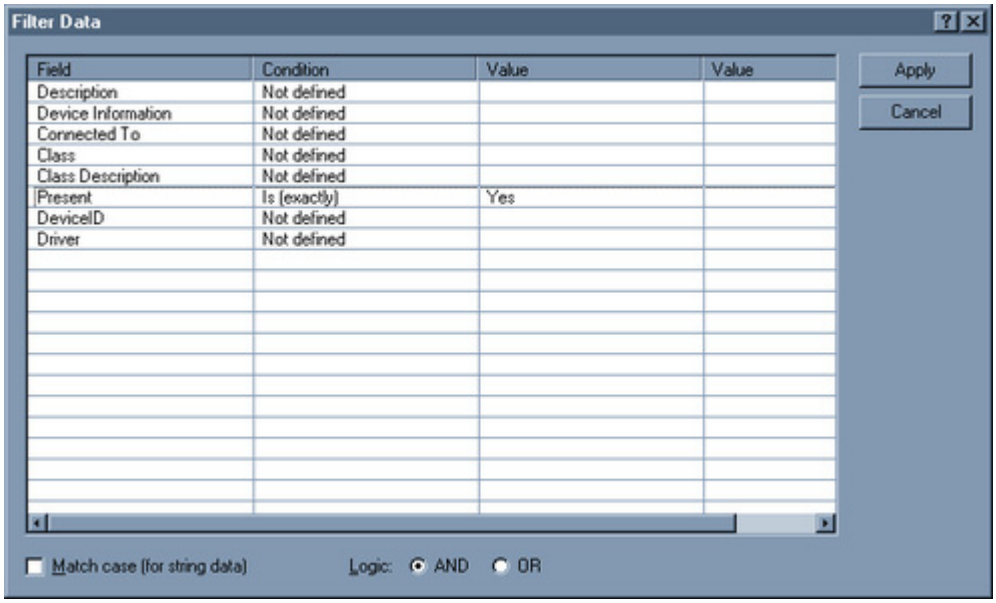
Filtering Data

DeviceLock Enterprise Manager provides very sophisticated data filtering, enabling you to narrow a scan or comparison result to only those data complying to your specific conditions.



To open the **Filter Data** dialog box, you can select **Filter** from the **View** menu or press the appropriate button on the **Main** toolbar.

Note: The window with a scan or comparison result must be active to use data filtering.



- The **Field** column contains all the fields available in the scan or comparison result that you want to filter. You can define the **AND**-**OR** logic for each field separately:

  AND – includes only those records that comply with all defined conditions. For example, Process = "explorer.exe" AND PID = 3764 retrieves all data where both the Process is "explorer.exe" and PID is 3764. It does not include data where the Process is "explorer.exe" and PID is not 3764 or where PID is 3764 but Process is not "explorer.exe".

  OR – includes all records that comply with at least one condition. For example, Process = "explorer.exe" OR PID = 3764 retrieves all data having one or both conditions, where Process = "explorer.exe" (no matter what PID is) or where PID is 3764 (no matter what Process is).

- The **Condition** column contains a list of logical operations that can be performed on a selected field. You can select only one logical operation for each field. DeviceLock Enterprise Manager supports two groups of logical operations, those for string data and non-string data.

  Logical operations that can be performed on string data (target string being the string you specify, for example, "Explorer.exe"):

  - **Is (exactly)** – selects only data having fields with strings that are identical to the target string.
  - **Includes** – selects only data having fields with strings that include a defined target string.
  - **Is not** – selects only data having fields with strings that are different from the target string.

- **Not includes** – selects only data having fields with strings that do not include the target string.
- **Empty** – selects only data having fields with empty strings.
- **Not Empty** – selects only data having fields with strings that are not empty.
- **Regular expression** – selects only data having fields with strings matching an expression. The expression may contain wildcards (for example, "explorer*").

If you want to narrow the search to the string's exact case (for example, "Explorer.exe" is different from "explorer.exe"), select the **Match case (for string data)** check box. Otherwise, case is ignored (for example, "Explorer.exe" and "explorer.exe" are identical).

Logical operations that can be performed on non-string data:

- **Equal to (=)** – selects data having field values that are identical to the defined value (for example, PID = 3764).
- **Greater than (>)** – selects data having field values that are greater than the defined value (for example, PID > 4).
- **Less than (<)** – selects data having field values that are less than the defined value (for example, PID < 4).
- **Not Equal to (!=)** – selects data having field values that are different from the defined value (for example, PID != 0).
- **Between (in)** – selects data having field values that are between the two defined values (for example, PID in 3000-4000).
- **Not Between (out)** – selects data having field values that are outside of the two defined values (for example, PID out 3000-4000).
- **Regular expression** – selects only data having field values matching an expression. The expression may contain wildcards (for example, 300*).

If you do not want to perform a logical operation for a field, select **Not defined** from the list of logical operations.

- **Value** columns contain user-defined arguments. The second **Value** column is used only when the **Between (in)** or **Not Between (out)** logical operation is selected. For all other logical operations only the first **Value** column is needed.

After you define a filtering expression, press the **Apply** button to start the filtering process.

You can save a filtered result in an external ANM file or export it to a text file (TXT and CSV) or MS Excel. select **Save As** from the **File** menu or press the appropriate button on the **Main** toolbar to save or export the filtered result.

As with any other DeviceLock Enterprise Manager file, filtered data can be opened and loaded into DeviceLock Enterprise Manager. To load a file, select **Open** from the **File** menu or press the appropriate button on the **Main** toolbar. Then specify the file you want to open. You can only load files that were previously saved by DeviceLock Enterprise Manager.

Content-Aware Rules for Devices (Regular Profile)

Content-Aware Rules extend the basic port/device access control functionality of DeviceLock DLP Suite by adding comprehensive, file-level protection of corporate documents containing confidential company information. Content-Aware Rules enable automatic content inspection of data copied to external storage devices, detection of sensitive content and enforcement of regulatory policies to ensure protection.

With Content-Aware Rules, you can selectively allow or deny access to specific file content regardless of preset permissions at the device type-level. You can also use Content-Aware Rules to allow or deny shadow copying of specific content, or to detect read, write or delete attempts of specific content without blocking/delaying access or creating shadow copies. For flexibility, Content-Aware Rules can be defined on a per-user or per-group basis.

You can configure Content-Aware Rules to apply to access control operations, to shadow copy operations, to detection operations, or to all of the above.

The following examples illustrate the use of Content-Aware Rules.

- **Example 1 – Using Content-Aware Rules for access control operations**. You can allow certain users or groups to read files containing the phrase "not for distribution" from Removable, Floppy, and Optical devices but prevent them from writing files containing more than one credit card number to Removable and Floppy devices.
- **Example 2 – Using Content-Aware Rules for shadow copy operations**. You can specify that only files containing credit card numbers, Social Security numbers, the words "Secret", "Confidential", "Restricted," and the phrases "Top Secret", and "For Official Use Only" will be shadow copied for security auditing and incident investigation purposes.

- **Example 3 – Using Content-Aware Rules for detection operations.** You can specify that only attempts to transfer files exceeding 20 Mb will be logged and alerted on, without blocking/delaying the transfer or creating shadow copies.

Note: You can define different online vs. offline Content-Aware Rules for the same user or sets of users. Online Content-Aware Rules (Regular Profile) apply to client computers that are working online. Offline Content-Aware Rules (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define offline Content-Aware Rules, see "Managing Offline Content-Aware Rules for Devices."

Content-Aware Rules can be applied to the following device types: Clipboard, Floppy, iPhone, MTP, Optical Drive, Palm, Printer, Removable, TS Devices, and Windows Mobile.

Note: When defining Content-Aware Rules for the Printer device type, consider the following:

- DeviceLock Service can perform content analysis of documents sent to print only if the **Spool print documents so program finishes printing faster** and **Start printing after last page is spooled** options are selected on the **Advanced** tab of the printer's **Properties** dialog box.

- File Type Detection content groups, Oracle IRM content groups and certain parameters (**File size**, **Modified**, **File name**, **Accessed by process**, **Password protected**, **Contains text** and **Additional parameters**) of Document Properties content groups are not applicable to documents sent to print.

Content-Aware Rules for Access Control Operations

When Content-Aware Rules apply to access control operations, they control read, write and delete operations for specified content. Delete and write operations are controlled together.

Content-Aware Rules allow you to do the following:

- Grant read/write access to specified file content when access is denied at the device type-level.
- Deny read/write access to specified file content when access is granted at the device type-level.

Note: DeviceLock can check access to devices at two levels: the interface (port) level and the type level. Some devices are checked at both levels, while others only at one level – either interface (port) or type. For example, a USB flash drive belongs to both levels: interface (USB) and type (Removable). Content-Aware Rules work only when access checking occurs at the type level (Removable, Floppy, etc.). DeviceLock does not perform the access check for USB devices at the type level if the following conditions are true:

- the device is not added to the USB Devices White List, **Access control for USB storage devices** is enabled in **Security Settings** and the user has no access to the **USB port** device type.
OR
- the device is added to the USB Devices White List and the **Control As Type** check box is cleared for it.

The following table provides summary information on access rights that can be specified in Content-Aware Rules.

ACCESS RIGHTS	DESCRIPTION
Generic: Read	Controls whether the user can read specified content from a device. Applies to the Optical Drive, Floppy, and Removable device types.
Generic: Write	Controls whether the user can write specified content to a device. Applies to the Floppy and Removable device types.

ACCESS RIGHTS	DESCRIPTION
Generic: Read, Write	Controls whether the user can read and write specified content from and to a device. Applies to the Floppy and Removable device types.
Generic: Copy to clipboard	Controls whether the user can paste specified content from the clipboard. Applies only to the Clipboard device type.
Generic: Print	Controls whether the user can print documents with specified content. Applies only to the Printer device type. *DeviceLock extracts and analyzes text from EMF, PostScript, PCL5, and PCL6 (PCL XL) print spooler formats*.
Generic: Clipboard Incoming Text	Controls whether the user can paste text data with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming File	Controls whether the user can paste files with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming Image	Controls whether the user can paste images with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming Unidentified Content	Controls whether the user can paste any other uncategorized data with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing Text	Controls whether the user can paste text data with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing File	Controls whether the user can paste files with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing Image	Controls whether the user can paste images with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing Unidentified Content	Controls whether the user can paste any other uncategorized data with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Encrypted: Read	Controls whether the user can read specified content from an encrypted device. Applies only to the Removable device type.
Encrypted: Write	Controls whether the user can write specified content to an encrypted device. Applies only to the Removable device type.
Encrypted: Read, Write	Controls whether the user can read and write specified content from and to an encrypted device. Applies only to the Removable device type.
Special Permissions: Copy Text	Controls whether the user can paste text data with specified content from the clipboard. Applies only to the Clipboard device type.

ACCESS RIGHTS	DESCRIPTION
Special Permissions: Copy Unidentified Content	Controls whether the user can paste any other uncategorized data with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy File	Controls whether the user can paste files with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy Image	Controls whether the user can paste images with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Screenshot	Controls whether the user can paste screenshots with specified content from the clipboard. Applies only to the Clipboard device type.

Note: Generic access rights specified for the Removable device type apply only to unencrypted devices. Encrypted access rights specified for the Removable device type apply only to encrypted devices. To specify access rights for both encrypted and unencrypted Removable devices, you must specify both Generic and Encrypted access rights. For detailed information on devices that are recognized by DeviceLock Service as encrypted devices, see "Encryption."

The following table shows how different device type-level and file-level permissions affect the state of a permission for a user account. Device type-level permissions are permissions set for a device type. File-level permissions are permissions defined by Content-Aware Rules.

	FULL ACCESS device type-level	**NO ACCESS** device type-level	**ALLOW READ/ DENY WRITE** device type-level
ALLOW READ file-level	allows read access to all content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read access to all but specified content, denies creation and renaming of empty folders and zero byte (0) files.	allows read access to all content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.
DENY READ file-level	denies read access to specified content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read and write access to all content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read access to specified content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.

	FULL ACCESS device type-level	**NO ACCESS** device type-level	**ALLOW READ/ DENY WRITE** device type-level
ALLOW WRITE file-level	allows write access to all content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies write access to all but specified content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies write access to all but specified content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.
DENY WRITE file-level	denies write access to specified content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read and write access to all content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.	denies write access to all content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.
ALLOW READ/ ALLOW WRITE file level	allows read and write access to all content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read and write access to all but specified content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	allows read access to all content, denies write access to all but specified content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.
DENY READ/ DENY WRITE file-level	denies read and write access to specified content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read and write access to all content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read access to specified content, denies write access to all content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.
ALLOW READ/ DENY WRITE file-level	allows read access to all content, denies write access to specified content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read access to all but specified content, denies write access to all content, denies creation and renaming of empty folders and zero byte (0) files.	allows read access to all content, denies write access to all content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.

	FULL ACCESS device type-level	**NO ACCESS** device type-level	**ALLOW READ/ DENY WRITE** device type-level
DENY READ/ ALLOW WRITE file-level	denies read access to specified content, allows write access to all content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read access to all content, denies write access to all but specified content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read access to specified content, denies write access to all but specified content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.
SHADOWING ALLOW/DENY file-level	allows read and write access to all content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies access to a device.	allows read access to all content, denies write access to all content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.
DETECTION ALLOW READ/ALLOW WRITE file-level	allows read and write access to all content, allows creation, deletion, and renaming of empty folders and zero byte (0) files.	denies read and write access to all content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.	allows read access to all content, denies write access to all content, denies creation, deletion, and renaming of empty folders and zero byte (0) files.

Note: If the No Access permission is set for a device type and there is a Content-Aware Rule that allows write access to certain content, auditing, alerting or content detection for the same device type, the Traverse Folder permission is granted to users for this device type. The Traverse Folder permission allows the user to move through folders and see files and folders located in subdirectories even if the user has no Read permission for the traversed folders.

When using Content-Aware Rules, consider the following:

- ***Content-Aware Rules with Deny settings take priority over rules with Allow settings if they apply to the same users or groups. Exception: Content-Aware Rules with Allow settings based on Document Properties group with Text extraction not supported flag enabled take priority over rules with Deny settings and allow transfer any matching content, including split (or multi-volume) archives.***
- ***Content-Aware Rules with Allow settings allow transfer of the whole data object (message or file, including archives and other containers) when the***

content matches these rules and when the content does not match a Content-Aware Rule with Deny settings.

- ***When users try to overwrite an existing file with a new file to which they are denied write access, the old file is deleted***. ***To prevent this, enable the*** Safe file overwrite ***parameter in Service Options.***
- ***When users try to modify a file to which they are denied write access, the file is deleted***. ***To prevent this, enable the*** Safe file overwrite ***parameter in Service Options***.
- ***When users open a file, modify it by inserting the content to which they are denied write access and then try to save changes, the file is deleted. To prevent this, enable the*** Safe file overwrite ***parameter in Service Options***.
- ***Unsafe removal of a device can result in the corruption of the device's file system and data***.
- ***When users try to copy files to which they are denied write access, these files are temporarily visible in Windows Explorer or other file manager applications. Actually, these files do not really exist on the target device, they are located in the memory cache and are removed from this cache immediately after DeviceLock finishes checking their content***.
- ***Checking the content of files can be a time-consuming operation. You cannot safely remove the device while this operation is in progress even if the copied files become visible in Windows Explorer or other file manager applications. In this situation, you receive an error message indicating that the device is currently busy***.
- ***Newly copied files cannot be opened for reading until DeviceLock finishes checking their content***.
- ***Checking the content of files can be a time-consuming operation. You can define a Content verification message to be displayed to users when content inspection is in progress. For detailed information on this message, see "***Content verification message***" in "Service Options"***.
- ***When users try to read or write files to which they are denied read or write access, they receive a DeviceLock Content-Aware blocked read or write message, if Content-Aware blocked read or write message is enabled in Service Options. For detailed information on these messages, see "***Content-Aware blocked read message***" and "***Content-Aware blocked write message***" in "Service Options"***.

Content-Aware Rules for Shadow Copy Operations

Before you can use Content-Aware Rules for shadow copy operations, you must turn on shadowing in **Auditing, Shadowing and Alerts** at the device type-level. Content-Aware Rules that apply to shadow copy operations filter the shadow copies of data and files written by the user.

The following table provides summary information on shadowing rights that can be specified in Content-Aware Rules.

SHADOWING RIGHTS	DESCRIPTION
Generic: Read	Controls whether or not data with specified content read from a device is shadow copied. Applies only to the MTP device type.
Generic: Write	Controls whether or not data with specified content written to a device is shadow copied. Applies to the Floppy, iPhone, MTP, Removable, Palm, and Windows Mobile device types.
Generic: Mapped Drives Write	Controls whether or not data with specified content written to a device is shadow copied. Applies only to TS Devices.
Generic: Print	Controls whether or not documents with specified content sent to printers are shadow copied. Applies to the Printer device type. *DeviceLock extracts and analyzes text from EMF, PostScript, PCL5, and PCL6 (PCL XL) print spooler formats*.
Generic: Copy to clipboard	Controls whether or not data with specified content pasted from the clipboard is shadow copied. Applies only to the Clipboard device type.
Generic: Clipboard Incoming Text	Controls whether or not text data with specified content pasted from the clipboard to a terminal session/virtual machine is shadow copied. Applies only to TS Devices.
Generic: Clipboard Outgoing Text	Controls whether or not text data with specified content pasted from the clipboard from a terminal session/virtual machine is shadow copied. Applies only to TS Devices.
Generic: Clipboard Incoming Image	Controls whether user attempts to paste images with specified content from the clipboard to a terminal session/virtual machine are shadow copied. Applies only to TS Devices.
Generic: Clipboard Outgoing Image	Controls whether user attempts to paste images with specified content from the clipboard from a terminal session/virtual machine are shadow copied. Applies only to TS Devices.
Generic: Clipboard Incoming File	Controls whether user attempts to paste files with specified content from the clipboard to a terminal session/virtual machine are shadow copied. Applies only to TS Devices.

SHADOWING RIGHTS	DESCRIPTION
Generic: Clipboard Outgoing File	Controls whether user attempts to paste files with specified content from the clipboard from a terminal session/virtual machine are shadow copied. Applies only to TS Devices.
Generic: Clipboard Incoming Unidentified Content	Controls whether or not any other uncategorized data with specified content pasted from the clipboard to a terminal session/virtual machine is shadow copied. Applies only to TS Devices.
Generic: Clipboard Outgoing Unidentified Content	Controls whether or not any other uncategorized data with specified content pasted from the clipboard from a terminal session/virtual machine is shadow copied. Applies only to TS Devices.
Encrypted: Write	Controls whether or not data with specified content written to an encrypted device is shadow copied. Applies only to the Removable device type.
Special Permissions: Write Calendar	Controls whether or not data with specified content written to a calendar on a mobile device from a PC is shadow copied. Applies to the iPhone, Palm, and Windows Mobile device types.
Special Permissions: Write Contact	Controls whether or not contacts with specified content written from a PC to a mobile device are shadow copied. Applies to the iPhone, Palm, and Windows Mobile device types.
Special Permissions: Write E-mail	Controls whether or not e-mail messages with specified content written from a PC to a mobile device are shadow copied. Applies to the iPhone, Palm, and Windows Mobile device types. For iPhone, this right controls shadow copying of e-mail account settings but not e-mail messages because iTunes does not support sync of messages.
Special Permissions: Write Attachment	Controls whether or not e-mail attachments with specified content written from a PC to a Windows Mobile or Palm device are shadow copied.
Special Permissions: Write Favorite	Controls whether or not favorites with specified content written from a PC to a Windows Mobile device or iPhone are shadow copied.
Special Permissions: Write File	Controls whether or not files with specified content written from a PC to a mobile device are shadow copied. Applies to the iPhone, Palm, and Windows Mobile device types.
Special Permissions: Write Media	Controls whether or not media data with specified content written using Windows Media Player to a Windows Mobile device from a PC and media files with specified content written to a Palm device and iPhone from a PC are shadow copied.
Special Permissions: Write Backup	Controls whether or not the iPhone backup data with specified content written from a PC to iPhone is shadow copied.
Special Permissions: Write Note	Controls whether or not notes with specified content written from a PC to a mobile device are shadow copied. Applies to the iPhone, Palm, and Windows Mobile device types.

SHADOWING RIGHTS	DESCRIPTION
Special Permissions: Write Pocket Access	Controls whether or not Pocket Access databases with specified content written from a PC to a Windows Mobile device are shadow copied.
Special Permissions: Write Task	Controls whether or not tasks with specified content written from a PC to a mobile device are shadow copied. Applies to the Palm and Windows Mobile device types.
Special Permissions: Write Expense	Controls whether or not Palm Expense application data with specified content written from a PC to a Palm device is shadow copied.
Special Permissions: Write Document	Controls whether or not Palm documents with specified content written from a PC to a Palm device are shadow copied.
Special Permissions: Write Unidentified Content	Controls whether or not any other uncategorized data with specified content written from a PC to a Windows Mobile device is shadow copied.
Special Permissions: Copy Text	Controls whether or not text data with specified content pasted from the clipboard is shadow copied. Applies only to the Clipboard device type.
Special Permissions: Copy Unidentified Content	Controls whether or not any other uncategorized data with specified content pasted from the clipboard is shadow copied. Applies only to the Clipboard device type.
Special Permissions: Copy File	Controls whether user attempts to paste files with specified content from the clipboard are shadow copied. Applies only to the Clipboard device type.
Special Permissions: Copy Image	Controls whether user attempts to paste images with specified content from the clipboard are shadow copied. Applies only to the Clipboard device type.
Special Permissions: Screenshot	Controls whether user attempts to paste screenshots with specified content from the clipboard are shadow copied. Applies only to the Clipboard device type.

Note: Generic shadowing rights specified for the Removable device type apply only to unencrypted devices. **Encrypted** shadowing rights specified for the Removable device type apply only to encrypted devices. To specify shadowing rights for both encrypted and unencrypted Removable devices, you must specify both **Generic** and **Encrypted** shadowing rights.

Content-Aware Rules for Detection Operations

When Content-Aware Rules apply to detection operations, they detect read, write, and delete attempts for specified content. Delete and write operations are controlled together.

The following table provides summary information on detection rights that can be specified in Content-Aware Rules.

DETECTION RIGHTS	DESCRIPTION
Generic: Read	Controls whether user attempts to read specified content from a device are detected. Applies to the Optical Drive, Floppy, and Removable device types.
Generic: Write	Controls whether user attempts to write specified content to a device are detected. Applies to the Floppy and Removable device types.
Generic: Read, Write	Controls whether user attempts to read and write specified content from and to a device are detected. Applies to the Floppy and Removable device types.
Generic: Copy to clipboard	Controls whether user attempts to paste specified content from the clipboard are detected. Applies only to the Clipboard device type.
Generic: Print	Controls whether user attempts to print documents with specified content are detected. Applies only to the Printer device type. *DeviceLock extracts and analyzes text from EMF, PostScript, PCL5, and PCL6 (PCL XL) print spooler formats*.
Generic: Clipboard Incoming Text	Controls whether user attempts to paste text data with specified content from the clipboard to a terminal session/virtual machine are detected. Applies only to TS Devices.
Generic: Clipboard Incoming File	Controls whether user attempts to paste files with specified content from the clipboard to a terminal session/virtual machine are detected. Applies only to TS Devices.
Generic: Clipboard Incoming Image	Controls whether user attempts to paste images with specified content from the clipboard to a terminal session/virtual machine are detected. Applies only to TS Devices.
Generic: Clipboard Outgoing File	Controls whether user attempts to paste files with specified content from the clipboard from a terminal session/virtual machine are detected. Applies only to TS Devices.
Generic: Clipboard Outgoing Image	Controls whether user attempts to paste images with specified content from the clipboard from a terminal session/virtual machine are detected. Applies only to TS Devices.
Generic: Clipboard Outgoing Text	Controls whether user attempts to paste text data with specified content from the clipboard from a terminal session/virtual machine are detected. Applies only to TS Devices.
Generic: Clipboard Incoming Unidentified Content	Controls whether user attempts to paste any other uncategorized data with specified content from the clipboard to a terminal session/virtual machine are detected. Applies only to TS Devices.

DETECTION RIGHTS	DESCRIPTION
Generic: Clipboard Outgoing Unidentified Content	Controls whether user attempts to paste any other uncategorized data with specified content from the clipboard from a terminal session/virtual machine are detected. Applies only to TS Devices.
Encrypted: Read	Controls whether user attempts to read specified content from an encrypted device are detected. Applies only to the Removable device type.
Encrypted: Write	Controls whether user attempts to write specified content to an encrypted device are detected. Applies only to the Removable device type.
Encrypted: Read, Write	Controls whether user attempts to read and write specified content from and to an encrypted device are detected. Applies only to the Removable device type.
Special Permissions: Copy Text	Controls whether user attempts to paste text data with specified content from the clipboard are detected. Applies only to the Clipboard device type.
Special Permissions: Copy Unidentified Content	Controls whether user attempts to paste any other uncategorized data with specified content from the clipboard are detected. Applies only to the Clipboard device type.
Special Permissions: Copy File	Controls whether user attempts to paste files with specified content from the clipboard are detected. Applies only to the Clipboard device type.
Special Permissions: Copy Image	Controls whether user attempts to paste images with specified content from the clipboard are detected. Applies only to the Clipboard device type.
Special Permissions: Screenshot	Controls whether user attempts to paste screenshots with specified content from the clipboard are detected. Applies only to the Clipboard device type.

Configuring Content Detection Settings

Content-Aware Rules are created based on content groups that enable you to centrally define types of content for which you want to control access. Content groups specify content filtering criteria that will be used to select data to which rules should be applied.

All content groups are stored in the Content Database. The same Content Database is used for both devices and protocols. The Content Database is a part of the DeviceLock Service policy and is also saved in an XML file with service settings that can be created using DeviceLock Management Console, DeviceLock Service Settings Editor, and DeviceLock Group Policy Manager.

There are several types of content groups: File Type Detection groups, Keywords groups, Pattern groups, Document Properties groups, Complex groups, and Oracle IRM groups. The sections below describe these groups and how to use them.

File Type Detection Content Groups

File Type Detection groups are used to control access to files based on file types. These groups contain definitions of the file types that make up these groups. A file type definition consists of two properties: a file name extension (for example, DOC) and a description (for example, Microsoft Word document). When you apply a rule based on a File Type Detection group, the rule is applied to all file types included in that group.

By defining rules based on File Type Detection groups, you can, for example, allow certain users or groups to read Word documents from Floppy devices but prevent them from writing Word documents to Floppy devices. You can deny read access to all executable files from Removable, Optical and Floppy devices but allow write access to all file types for Removable and Floppy devices. You can also specify that only Word, Excel, and PDF documents will be shadow copied.

DeviceLock includes more than 30 predefined (built-in) File Type Detection groups that you can use to set up the desired configuration of permissions and/or shadow copy operations. You can use the built-in content groups as they are, create their editable copies (duplicates) or create your own content groups to suit your particular organization's needs.

The following table lists these predefined content groups:

BUILT-IN FILE TYPE DETECTION GROUPS	
Android	MS Outlook, Outlook Express & Email archives
Archives	MS PowerPoint
Audio, Video & Flash	MS Project
BlackBerry	MS Publisher
Common Object File Format (COFF)	MS Visio
Database	MS Windows Installer
Executable	MS Windows Memory Dump
Fax Documents	MS Word
FileMaker Pro	MS Works
Fonts	OpenOffice, StarOffice, OpenDocument, etc.
Help Files	Oracle IRM
Images, CAD & Drawing	PDF, PostScript, & XPS Documents
iOS	QuickBooks, Quicken, TurboTax & etc.
Lotus SmartSuite	Rich Text Format
MS Access	Security Certificates
MS Excel	Text, HTML & XML
MS InfoPath	Virtual Machines
MS Money	WordPerfect Office
MS OneNote	

Note: Content-Aware Rules support Word To Go, Sheet To Go, and Slideshow To Go formats for Palm devices. Word To Go format is included in the MS Word and Rich Text Format built-in content groups, Sheet To Go format is included in the MS Excel built-in content group, while Slideshow To Go format is included in the MS PowerPoint built-in content group.

Microsoft Word or Rich Text Format (RTF) files, Excel files and PowerPoint files can be transferred to a Palm device using the Documents To Go application. The Documents To Go application converts these

files to special formats: Word and RTF files are converted to Word To Go format, Excel files are converted to Sheet To Go format, while PowerPoint files are converted to Slideshow To Go format. The converted files are automatically downloaded to the Palm when users synchronize.

With built-in content groups, you can quickly create and apply rules without having to define your own content groups.

Note: You can view file type definitions that are included in the built-in File Type Detection groups but you cannot edit or delete them. For information on how to view the built-in content groups, see "Viewing Built-in Content Groups."

Creating Custom File Type Detection Groups

You can define Content-Aware Rules based on your own (custom) content groups if the predefined content groups included with DeviceLock do not meet your requirements. Custom File Type Detection content groups enable you to specify any file types that you want in the same group to better meet your individual business needs.

For example, suppose you need to grant certain users access to Word, Excel, PDF documents and graphic files. To do this, first you create a new File Type Detection content group that represents these document content types. Then you define a rule based on this custom content group.

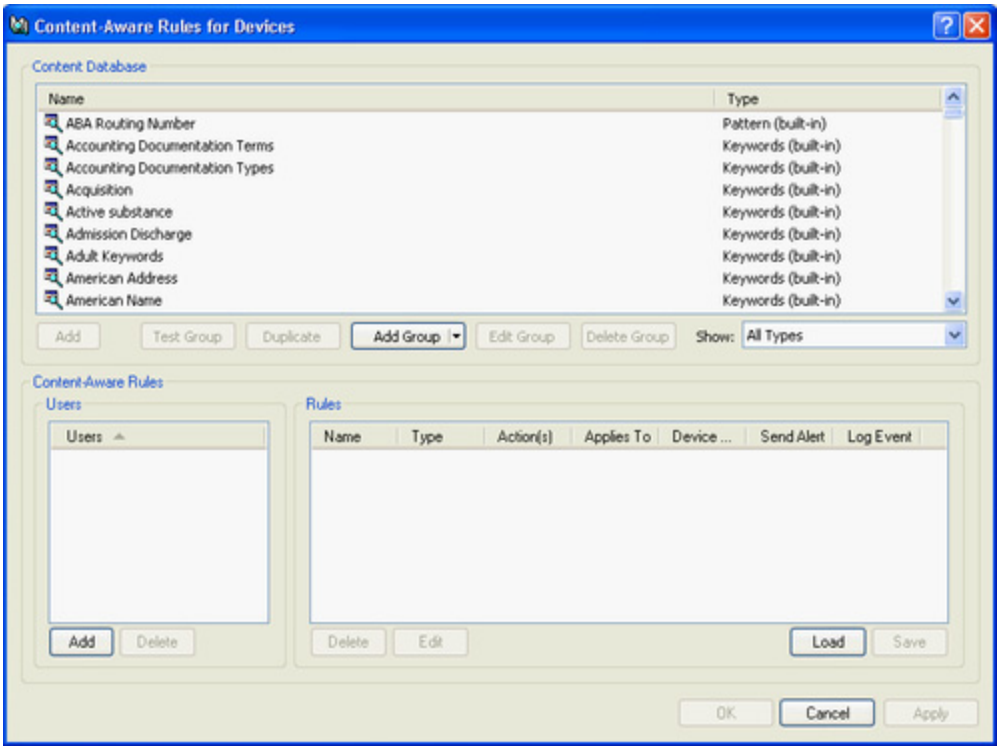
To create a custom File Type Detection group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

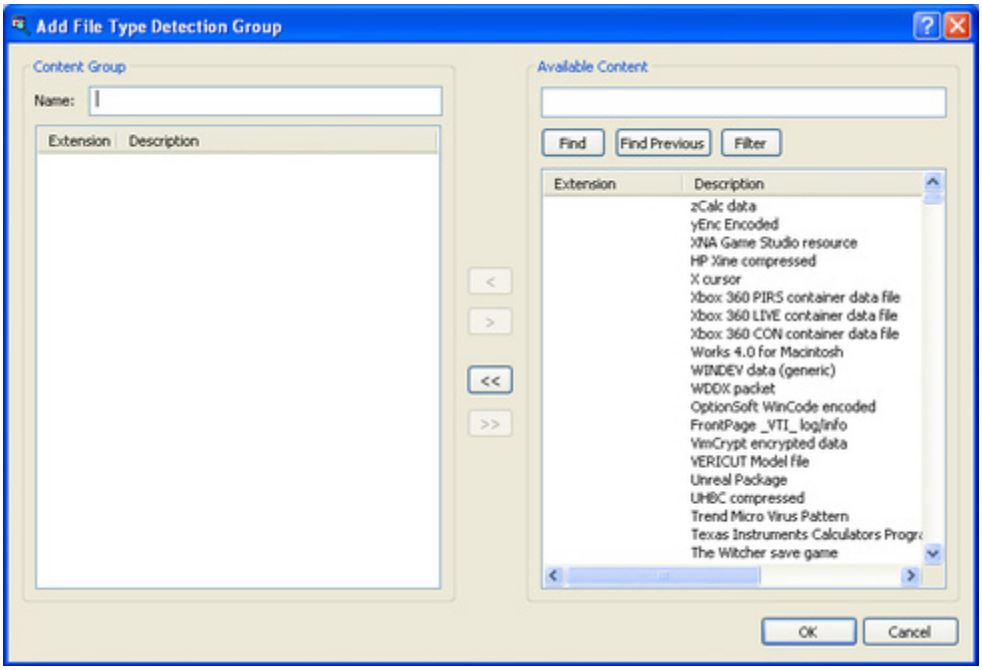
   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Devices dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **File Type Detection**.

   The Add File Type Detection Group dialog box appears.



5. In the left pane of the **Add File Type Detection Group** dialog box, under **Content group**, type the name of the new content group in the **Name** box.

6. In the right pane of the **Add File Type Detection Group** dialog box, under **Available Content**, select any file type you want to add to the new content group, and then click the left single-arrow button <.

   You can select multiple file types by holding down the SHIFT key or the CTRL key while clicking them.

   To remove single file types from the content group, use the right single-arrow button >. To add or remove all available file types to or from the content group at the same time, use the left double-arrow button << or right double-arrow button >>.

   Note: You can search the available content database for specific file types by extension or description. You can use wildcards such as asterisks (*) and question marks (?) to search for a specific group of file types. To find a specific file type or specific group of file types, under **Available Content**, type an extension or description with or without wildcards in the search string, and then click **Find**. To filter file types, click **Filter**. To remove the filter, apply it to an empty string.

   An asterisk (*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity.

7. Click **OK** to close the **Add File Type Detection Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Devices dialog box.

Keywords Content Groups

Keywords groups are used to control access to files based on whether certain words or phrases occur in a document.

By defining rules based on Keywords groups, you can, for example, allow read access to all documents containing the phrases “Top Secret” and “For Official Use Only” from Removable, Floppy and Optical devices but deny write access to Removable and Floppy devices for these documents. You can also specify that only documents containing the phrases “Top Secret” and “For Official Use Only” will be shadow copied.

DeviceLock includes more than 160 predefined (built-in) Keywords groups that you can use to set up the desired configuration of permissions and/or shadow copy operations. You can use the built-in content groups as they are, create their editable copies (duplicates) or create your own content groups to suit your particular organization’s needs.

The following table lists these predefined content groups:

BUILT-IN KEYWORDS GROUPS	
Accounting Documentation Terms	Production Charges
Accounting Documentation Types	Profanity
Acquisition	Profiles
Active substance	Profit Loss
Admission Discharge	Project Names
Adult Keywords	Project Release Dates
American Address	Property

BUILT-IN KEYWORDS GROUPS

American Name	Racism Keywords
Bank ABA	Resume
Bank ACNT	Russian: Account Statement
Bank STMT	Russian: Accounting Documentation
Board Meeting	Russian: Accounting Documentation Terms
Breach of Obligation	Russian: Accounting Documentation Types
Breach of Standards	Russian: Bank Account
Breach of the Law	Russian: Bank Operations
Business Documentation	Russian: Banking Operations Participants
Business Documentation Terms	Russian: Breach of Commitment
Business Documentation Types	Russian: Breach of Law
Business Rivals	Russian: Business Documentation
Business Trips & Meetings	Russian: Business Documentation Terms
C# Source Code	Russian: Business Documentation Types
C/C++ Source Code	Russian: Business Partners
Cellular Operator Call Log	Russian: Business Trips & Meetings
COBOL Source Code	Russian: Company Development Plan
Common Disease	Russian: Compensation and Benefits
Common Medical Terms	Russian: Confidential Information
Company Development	Russian: Corporate Capital
Compensation and Benefits	Russian: Corporate Property
Compliance Report	Russian: Expenses
Confidential	Russian: Failures
Confidential Partners Information	Russian: Financial Information
Credit Report	Russian: Financial Report
Credits	Russian: Financial Terms
Discontent	Russian: Firing
Discrediting Information	Russian: Innovations
Driver’s License	Russian: Insurance
Employer Identification Number	Russian: Internal Payments
Ethnicity	Russian: Investors and Investments
Executive Job Searches	Russian: Labor Law
Failures	Russian: Loans and Credits
Financial Report	Russian: Manufacturing
Financial Statements	Russian: Market Development Plan
Firing	Russian: Medicinal Active Substances
FITS Date & Time	Russian: Medicinal Drugs
FITS File Checksum	Russian: Noncompliant
FITS File Descriptors	Russian: Passwords and Access Codes
FITS Hierarchical file grouping	Russian: Physical Security
FITS Instrumentorum	Russian: Prices
FITS Non-standard	Russian: Project Documentation
FITS Observations	Russian: Project Names
FITS Standard	Russian: Project Versions
Gambling	Russian: Projects Release Date
Grades	Russian: Technology
HCFA (CMS) 1500 Form	Russian: User Names
HIPAA - Diseases	Russian: Working Conditions
HIPAA HCPCS	Sales Forecast
HIPAA ICD 10 - Diseases and Injuries	Sarbanes-Oxley Sensitive
HIPAA ICD 10 - Drugs and Chemicals	Security
HIPAA ICD9	Security Agencies
HIPAA NDC Classes	Sensitive Disease
HIPAA NDC Dosages	Sexual Language
HIPAA NDC Listing	Social Security
HIPAA NDC Routes	SPAM

BUILT-IN KEYWORDS GROUPS	
Illegal Drugs	Prices
Innovations	Pro Earnings
Internet Slang Abbreviations	Sports
Investments	Staff Training
Java Source Code	Substance Abuse
Japan: Surname in Hiragana	Suspicious Activity Report
Japan: Surname in Kanji	Technology
Japan: Surname in Katakana	UBO4 Form
Japan: Surname in One-Byte-Katakana	US Birth Date
Market Development	US Birth Place
Medical Diagnosis	US Expiry Date
Medical Record Numbers	User Name
MEMO	VB Source Code
Network Security	Violence
Partner Names	Weapon Keywords
Password	Wire Transfer
Payments	Working Conditions
PCI GLBA	
Perl Source Code	
Price List	

With built-in content groups, you can quickly create and apply rules without having to define your own content groups.

Note: You can view keywords that are included in the built-in Keywords groups but you cannot edit or delete them. For information on how to view the built-in content groups, see "Viewing Built-in Content Groups."

Creating Custom Keywords Groups

You can define Content-Aware Rules based on your own (custom) content groups if the predefined content groups included with DeviceLock do not meet your requirements. Custom Keywords content groups enable you to specify any keywords that you want in the same group to better meet your individual business needs.

To create a custom Keywords group

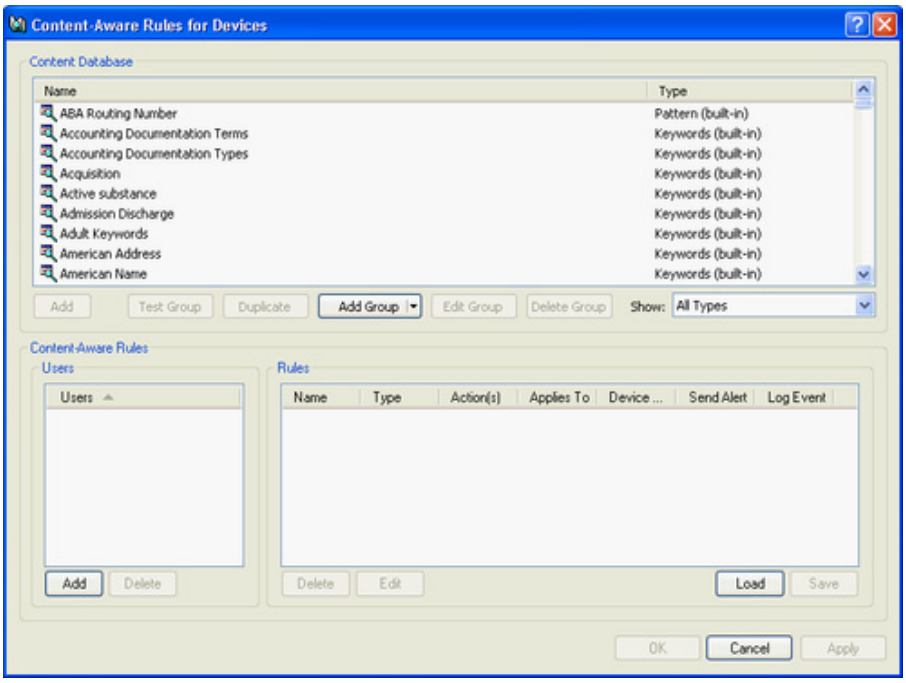
1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.

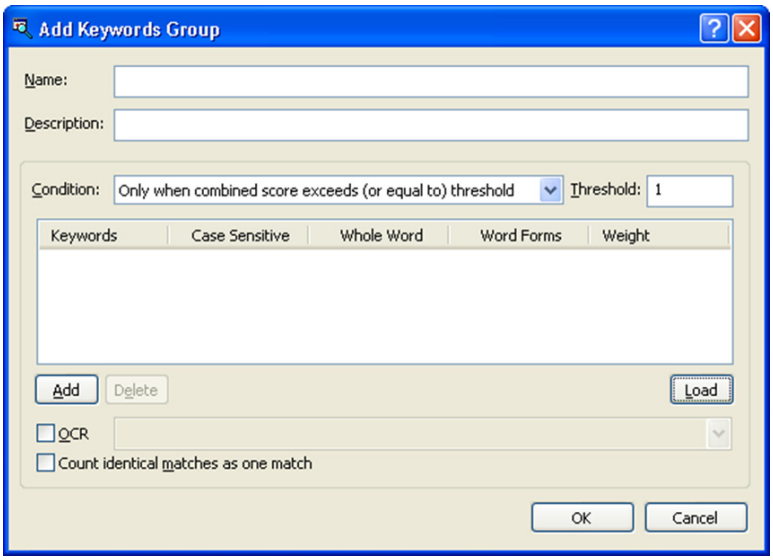
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

The Content-Aware Rules for Devices dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Keywords**.

   The Add Keywords Group dialog box appears.



5. In the **Add Keywords Group** dialog box, do the following:

USE THIS	TO DO THIS
Name	Specify the name of the group.
Description:	Specify a description for the group.
Condition:	Specify conditions for firing rules associated with this content group. To do so, in the **Condition** list, click any of the following options: • **Match any keyword(s)** indicates that a rule associated with this content group is activated every time any of the specified keywords is found within text data. • **Match all keyword(s)** indicates that a rule associated with this content group is activated every time all of the specified keywords are found within text data. • **Only when combined score exceeds (or equal to) threshold** indicates that a rule associated with this content group is activated every time the total number (sum) of occurrences of all found keywords within text data equals or exceeds the threshold number of occurrences of the keywords.
Threshold	Specify the threshold number of occurrences of the keywords. This number can range from 0 to 65535. This property requires a value if you selected the **Only when combined score exceeds (or equal to) threshold** option.
Keywords	Specify words and phrases that must occur within text data. Double-click under **Keywords** to enter a keyword or phrase.
Case Sensitive	Determine the case sensitivity of the keywords. Select the **Case Sensitive** check box to specify a case-sensitive comparison of the keywords (for example, the words "test" and "Test" will be treated as different keywords.). Clear the **Case Sensitive** check box to specify a case-insensitive comparison of the keywords (for example, the words "test" and "Test" will be treated as the same keyword).
Whole Word	Specify keyword matching options. Select the **Whole Word** check box to specify the exact match option (allows you to find an exact match of your keyword). Clear the **Whole Word** check box to specify the broad match option (allows you to find all grammatical variations of your keyword).
Word Forms	Specify keyword morphology (linguistics) search options. Select the **Word Forms** check box to enable morphology search for Catalan, English, French, German, Italian, Polish, Portuguese, Russian, and Spanish languages. Also, it enables search support for Russian transliterated words. *The keyword morphology search can be time-consuming and resource-intensive.* Clear the **Word Forms** check box to disable morphology and transliterated search.
Weight	Specify the degree of importance for each keyword or phrase. Weight is used to count the number of occurrences of the specified keywords within text data. This property requires a value if you selected the

USE THIS	TO DO THIS
	Only when combined score exceeds (or equal to) threshold option. Possible values: **Heavy**, **Above Normal**, **Normal** (default value), **Below Normal**, **Light**. These weight values are interpreted as follows: • **Heavy** weight indicates that each keyword occurrence is counted as three occurrences. This value is the highest. • **Above Normal** weight indicates that each keyword occurrence is counted as two occurrences. • **Normal** weight indicates that each keyword occurrence is counted as one occurrence. • **Below Normal** weight indicates that two keyword occurrences are counted as one occurrence. • **Light** weight indicates that three keyword occurrences are counted as one occurrence. This value is the lowest.
Add	Specify keywords and phrases. Click **Add** to enter a keyword or phrase.
Delete	Delete a keyword. To do so, select the keyword you want to delete, and then click **Delete**. You can select multiple keywords by holding down the SHIFT key or the CTRL key while clicking them.
Load	Import a list of keywords from a tab-delimited text file.
OCR	Extract text from images for further checking against the list of keywords defined in this content group. To do so, select the **OCR** check box and up to 8 languages. For optimal performance and recognition quality, we recommend that you select only those languages that are really needed.
Count identical matches as one match	Combine duplicate matches returned by the regular expression into a single match. To do so, select the **Count identical matches as one match** check box. This parameter is active when the **Only when combined score exceeds (or equal to) threshold** option is selected.

6. Click **OK** to close the **Add Keywords Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Devices dialog box.

Pattern Content Groups

Pattern groups let you control access to text files using patterns of text described by Perl regular expressions. Patterns provide a flexible and powerful way to automatically detect potentially sensitive content (for example, credit card numbers, Social Security numbers, e-mail addresses, and phone numbers) within documents. For more information on creating

and using Perl regular expressions, refer to the Perl regular expressions quick start tutorial and Perl regular expressions tutorial.

By defining rules based on Pattern groups, you can, for example, prevent certain users or groups from writing documents containing credit card numbers to Removable and Floppy devices. You can also turn off shadow copying of documents that do not contain credit card numbers.

DeviceLock includes more than 75 predefined (built-in) Pattern groups that you can use to set up the desired configuration of permissions and/or shadow copy operations. You can use the built-in content groups as they are, create their editable copies (duplicates) or create your own content groups to suit your particular organization's needs.

The following table lists these predefined content groups:

BUILT-IN PATTERN GROUPS	
ABA Routing Number	Russian: Classification of Enterprises and Organizations
American Name (Ex)	Russian: Driver's License Number
Austria SSN	Russian: Health Insurance Number
BIC (ISO 9362)	Russian: International Passport
Californian ID Number	Russian: Main State Registration Number
Canadian Postal Code	Russian: Motorcycle Numbers
Canadian Social Insurance Number	Russian: Passport
China National ID	Russian: Pension Insurance Number
Credit Card Number	Russian: Post Code
Danish Personal ID	Russian: Taxpayer Identification Number
Dollar Amount	Russian: Telephone Number
Dominican Republic ID Number	Russian: Trailer Numbers
Email Address	Russian: Vehicle Registration Document
European VAT Number	Scotland CHI
Finnish ID	South African ID Number
France INSEE Code	South Korean Resident Registration Number
French NINO	Spanish DNI
German eTIN	Spanish Full Name
German Telephone Number	Spanish NIF
GPS Data (RMC String)	Spanish SSN
Health Insurance Claim	SQL Queries
IBAN	Sweden Personal ID
International Telephone Number	Sweden Phone Number
IP Address	Sweden Post Code
Irish PPSN	Taiwan: ID Number
Irish VAT	Taiwan: Jih Sun Bank Account Number
ISO Date	TCP/UDP Port Number
Japan: Address	Time (12/24h)
Japan: Date	Turkish ID Number
Japan: Phone Number	UK Date
Japan: Social Security and Tax Number System	UK National Insurance Number
MAC Address	UK NHS Number
Mexican Tax ID Number	UK Phone Number
Microsoft Windows Product Key	UK Post Code
National Provider Identifier	UK RD&E Hospital Number
Norwegian Birth Number	UK Tax Code

BUILT-IN PATTERN GROUPS	
Poland National Identity Card Number Polish ID Number RAMQ ROK Registration Number Russian: Address Russian: Auto Insurance Number Russian: Bank Account Number Russian: BIC Russian: Car Numbers Russian: Classification of Economic Activities	Uniform Resource Locator (URL) US Date US Phone Number US Social Security Number US Zip Code US/UK Home Address VIN

With built-in content groups, you can quickly create and apply rules without having to define your own content groups.

Note: You can view regular expression patterns that are included in the built-in Pattern content groups but you cannot edit or delete them. For information on how to view the built-in content groups, see "Viewing Built-in Content Groups."

Creating Custom Pattern Groups

You can define Content-Aware Rules based on your own (custom) content groups if the predefined content groups included with DeviceLock do not meet your requirements. Custom content groups enable you to specify any pattern that you want to use to identify sensitive information within documents.

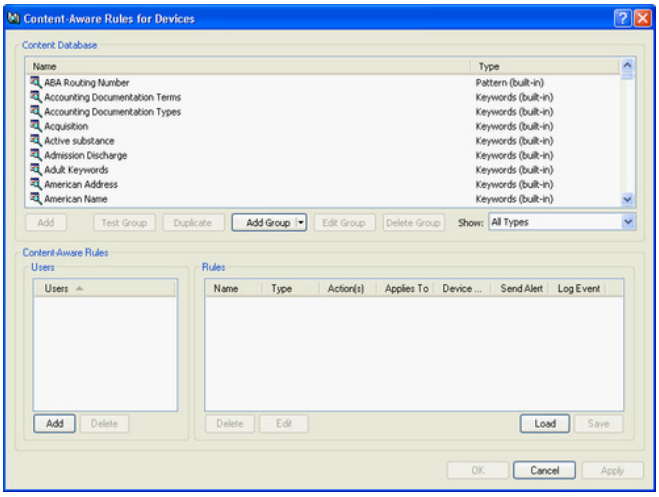
To create a custom Pattern group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

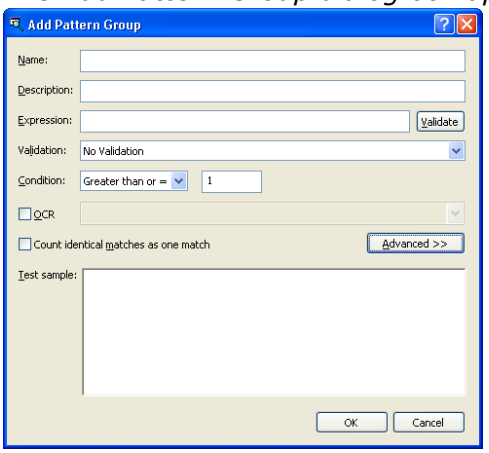
   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

The Content-Aware Rules for Devices dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Pattern**.

   The Add Pattern Group dialog box appears.



5. In the **Add Pattern Group** dialog box, do the following:

USE THIS	TO DO THIS
Name	Specify the name of the group.
Description:	Specify a description for the group.
Expression	Specify a pattern by creating a regular expression. For information on how to create Perl regular expressions, refer to the Perl regular expressions quick start tutorial and Perl regular expressions tutorial.
Validate	Check regular expression syntax.

USE THIS	TO DO THIS
Validation	Perform the actual validation on the potential matches returned by the regular expression. The following options are available: **No validation** (this option is selected by default), **ABA Routing Number**, **American Name (Ex)**, **Austria SSN**, **Canadian Social Insurance Number**, **China National ID**, **Credit Card Number (All)**, **Credit Card Number (American Express)**, **Credit Card Number (Diners Club)**, **Credit Card Number (Diners Club En Route)**, **Credit Card Number (Diners Club Carte Blanche), Credit Card Number (Discover)**, **Credit Card Number (JCB)**, **Credit Card Number (Laser)**, **Credit Card Number (Maestro)**, **Credit Card Number (Master Card)**, **Credit Card Number (Solo)**, **Credit Card Number (Switch)**, **Credit Card Number (Visa)**, **Credit Card Number (Visa Electron)**, **Danish Personal ID**, **Date, Date (ISO)**, **Dominican Republic ID**, **Email Address**, **European VAT Number**, **Finnish ID**, **France INSEE Code**, **German eTIN**, **Health Insurance Claim**, **IBAN**, **IP Address**, **Irish PPSN**, **LUHN Checksum**, **Norwegian Birth Number**, **NPI**, **Polish ID**, **Quebec Healthcare Medical Number, Mexican Tax Id Number, Polish National Identity Card, ROK Registration Number**, **Russian Bank Account Number**, **Russian Health Insurance Number**, **Russian Taxpayer Identification Number**, **Russian Main State Registration Number**, **Russian Classification Of Enterprises And Organizations, South African Id Number, South Korean Resident Registration Number, Japan: Social Security and Tax Number System, Spanish NIF, Taiwan ID, Turkish Id Number, UK NHS Number**, **UK National Insurance Number**, **UK Phone Number**, **UK Post Code**, **UK Tax Code**, **URL**, **US Social Security Number**.
Condition:	Specify conditions for firing rules associated with this content group. To do so, in the **Condition** list, click any of the following options: • **Less than or =** indicates that a rule associated with this content group is activated every time the number of matches returned by the regular expression is less than or equal to the specified number. • **Equal to** indicates that a rule associated with this content group is activated every time the number of matches returned by the regular expression is equal to the specified number. • **Greater than or =** indicates that a rule associated with this content group is activated every time the number of matches returned by the regular expression is greater than or equal to the specified number. • **Between** indicates that a rule associated with this content group is activated every time the number of matches returned by the regular expression is within the specified range.
OCR	Extract text from images for further checking against the regular expression defined in this content group. To do so, select the **OCR** check box and up to 8 languages. For optimal performance and recognition quality, we recommend that you select only those languages that are really needed.
Count identical matches as	Combine duplicate matches returned by the regular expression into a single match. To do so, select the **Count identical matches as one**

USE THIS	TO DO THIS
one match	**match** check box.
Advanced	Quickly test your regular expression pattern on sample data. Click **Advanced** to display or hide the **Test sample** box.
Test sample	Enter a test string and view the result. DeviceLock supports real-time color highlighting of test results. All matches are highlighted in green, while strings that do not match the pattern are highlighted in red.

6. Click **OK** to close the **Add Pattern Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Devices dialog box.

Document Properties Content Groups

Document Properties groups are used to control access to files based on file properties such as file name, size, etc. You can also use a Document Properties content group to control access to password-protected documents and archives as well as text images.

Note: The AND logic is applied to all file properties specified within a Document Properties group. For example, if you want to control access to files larger than 5 megabyte (MB) in size and password-protected documents and archives, you should create two separate Document Properties groups: one group for files larger than 5 MB in size and another group for password-protected documents and archives. If you specify these file properties within the same Document Properties group and then create a Content-Aware Rule based on this content group, this rule will control password-protected documents and archives that are larger than 5 MB.

By defining rules based on Document Properties groups, you can, for example, allow read access to all documents larger than 1 MB in size from Removable, Floppy and Optical devices but deny write access to Removable and Floppy devices for these documents. You can also specify that only documents whose size exceeds 5 MB will be shadow copied.

There are no predefined (built-in) Document Properties content groups to use. The following procedure describes how to create your own Document Properties group.

To create a Document Properties group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

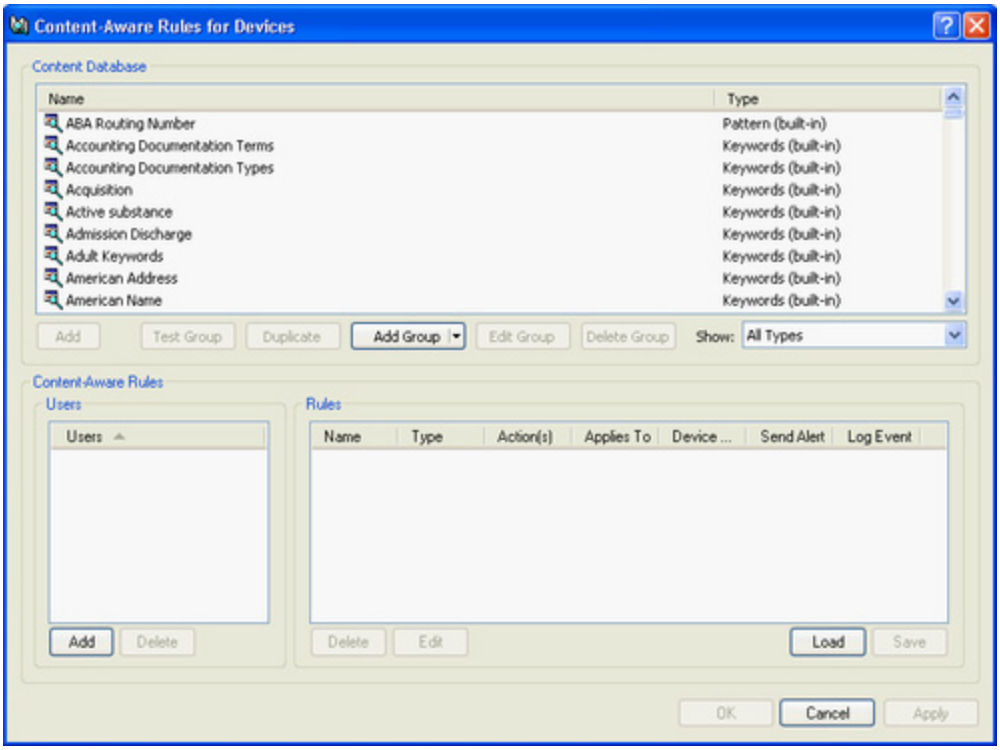
   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

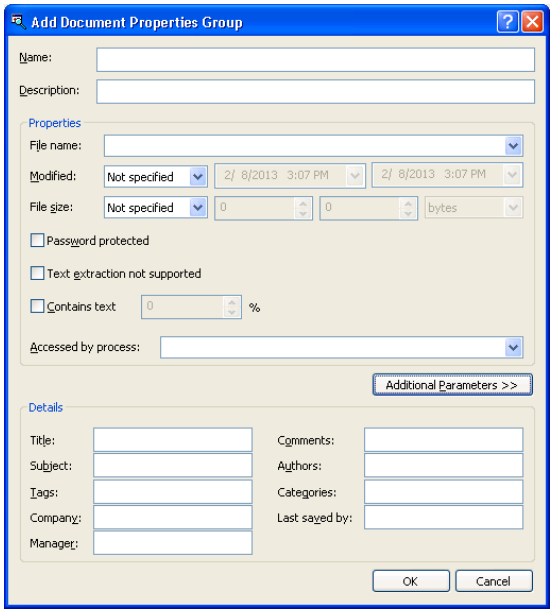
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

The Content-Aware Rules for Devices dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Document Properties**.

   The Add Document Properties Group dialog box appears.



5. In the **Add Document Properties Group** dialog box, do the following:

USE THIS	TO DO THIS
Name	Specify the name of the group.
Description:	Specify a description for the group.
File name	Specify the file names. You can use wildcards, such as asterisks (*) and question marks (?). For example, type ***.txt** to specify all files that have the .txt extension. Multiple file names must be separated by a semicolon (;), for example, ***.doc; *.docx**. *An asterisk (*) replaces an unlimited number of characters. The question mark (?) replaces a single character*. **Note:** For shadowing data captured from the Printer device type, the file name value you specify is compared with names provided in the **File Name** column of the Shadow Log Viewer.
Modified	Specify the last modification date/time of the file. To do so, in the **Modified** list, click any of the following options: • **Not specified** (this option is selected by default) • **Before than** indicates that the file's modified date/time must be earlier than the specified date/time. • **After than** indicates that the file's modified date/time must be later than the specified date/time. • **Between** indicates that the file's modified date/time must fall within the specified date/time range. • **Not older than** indicates that the file's modified date/time must not be older than the specified number of seconds, minutes,

USE THIS	TO DO THIS
	days, weeks, months, and years. • **Older than** indicates that the file's modified date/time must be older than the specified number of seconds, minutes, days, weeks, months, and years.
File size	Specify the file size in bytes, kilobytes, megabytes, gigabytes or terabytes. To do so, in the **File size** list, click any of the following options: • **Not specified** (this option is selected by default) • **Equal to** indicates that the file(s) must have a size that is equal to the size you specify. • **Less than** indicates that the file(s) must have a size that is less than the size you specify. • **More than** indicates that the file(s) must have a size that is more than the size you specify. • **Between** indicates that the file size must fall within the specified range.
Password protected	Detect and control access to password-protected archives, PDF files, and Microsoft Office documents (.doc, .xls, .ppt, .docx, .xlsx, .pptx). If you select the **Password protected** check box for a Document Properties group and then create a Content-Aware Rule based on this content group, this rule will control access to password-protected archives, PDF files, and Microsoft Office documents. Clear the **Password protected** check box if you do not want to detect and control access to password-protected archives, PDF files, and Microsoft Office documents. For information on the supported archive formats, see the description of the "Inspection of files within archives" feature.
Text extraction not supported	Control access to unsupported file formats. If you select the **Text extraction not supported** check box for a Document Properties group and then create a Content-Aware Rule based on this content group, this rule will control access to all files in an unsupported format. All supported file formats are listed in the "Extending DeviceLock Functionality with ContentLock and NetworkLock" section. You can use this parameter to allow transfer of split (or multi-volume) .cab or .rar archives that cannot be unpacked and analyzed by default in case there are active content-aware rules combined with **Archives content inspection on read** or **Archives content inspection on write** options enabled in **Service options**. Allow Content-Aware Rules based on Document Properties group with **Text extraction not supported** flag enabled take priority over deny rules and allow transfer any matching content, including split (or multi-volume) archives.
Contains text	Detect and control access to images based on whether or not they contain text. If you select the **Contains text** check box for a Document Properties group and then create a complex Content-Aware Rule based on this content group and the built-in Images, CAD & Drawing content group (File Type Detection) combined by the AND operator, this rule will check whether supported image files contain text and control access to text images. Clear the **Contains text** check box if you do not want to detect and control access to text images. For

USE THIS	TO DO THIS
	information on the supported image files, see the description of the "Text in picture detection" feature. If you select the **Contains text** check box, specify the amount of text that images must contain. The amount of text is expressed as a percentage of the total image area. For example, if text occupies ½ of the image, the amount of text makes 50%. If an image contains only text, the amount of text is 100%. **Note:** The **Contains text** option also applies to other supported file formats. In this case, the percentage means the ratio of the text size in characters to file size in bytes.
Accessed by process	Specify the name of the process accessing the document's file. You can use wildcards, such as asterisks (*) and question marks (?). Multiple process names must be separated by a semicolon (;), for example, **explorer.exe; notepad.exe**.
Additional Parameters	Specify some additional textual parameters supported only for compound documents and new MS Office files (.docx, .xlsx, .pptx). The AND logic is applied to all specified fields. You can use wildcards, such as asterisks (*) and question marks (?). Multiple values must be separated by a semicolon (;), for example, **john; mik***.

6. Click **OK** to close the **Add Document Properties Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Devices dialog box.

Complex Content Groups

Complex groups use Boolean expressions to select documents for which you want to control access. These groups can include any combination of built-in or custom content groups (File Type Detection, Keywords, Pattern, and Document Properties groups) linked with any number of the standard logical operators. Each content group is treated as a single filter criterion that can be included in your Boolean expression. By using multiple content groups, you can create complex filters to identify sensitive content contained in documents.

The following table lists the logical operators in order of precedence from highest to lowest.

OPERATOR	MEANING
NOT	Logical negation of a filter criterion
AND	Both filter criteria must apply
OR	Either filter criterion can apply

You can use parentheses to modify the precedence of operators and force some parts of an expression to be evaluated before others. Nested criteria enclosed in parentheses are

evaluated in inner-to-outer order. Multiple levels of nesting are supported. A complex group can contain a maximum of 50 content groups.

There are no predefined (built-in) Complex content groups to use. The following procedure describes how to create your own Complex group.

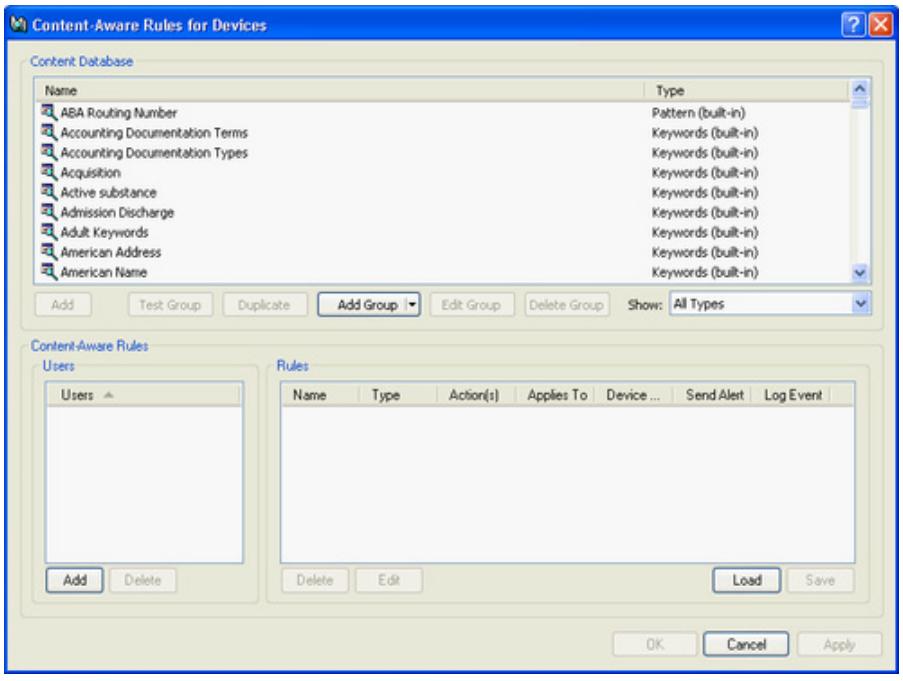
To create a Complex group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

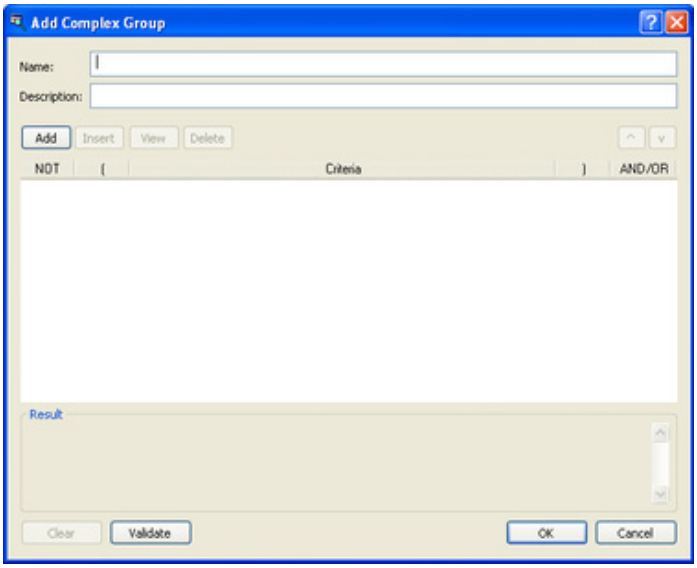
   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Devices dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Complex**.

   The Add Complex Group dialog box appears.



5. In the **Add Complex Group** dialog box, do the following:

USE THIS	TO DO THIS
Name	Specify the name of the group.
Description:	Specify a description for the group.
Add	Add the desired content groups from the Content Database. To do so, click **Add** to open the **Content Groups** dialog box. In the **Content Groups** dialog box, under **Content Database**, select the desired content group, and then click **OK**. *You can select multiple content groups by holding down the SHIFT key or the CTRL key while clicking them.* *To view information about a content group, select the desired group, and then click View Group*. *The content groups you added appear in the Criteria column in the Add Complex group dialog box. Each content group you add is treated as a single filter criterion that can be included in your Boolean expression*.
Insert	Insert a content group from the Content Database before the currently selected group in the **Criteria** column. To do so, click **Insert** to open the **Content Groups** dialog box. In the **Content Groups** dialog box, under **Content Database**, select the desired content group, and then click **OK**.
View	View information about the currently selected group in the **Criteria** column.
Delete	Delete the selected group from the **Criteria** column.

USE THIS	TO DO THIS
NOT	Join each content group you select with the logical NOT operator. To do so, select the desired group in the **Criteria** column, and then select the appropriate check box in the **Not** column.
AND/OR	Join each content group you select with the logical AND or OR operator. To do so, select the desired group in the **Criteria** column, and then click either **AND** or **OR** in the appropriate list in the **AND/OR** column.
Clear	Clear the current list of content groups in the **Criteria** column.
Validate	Validate your expression. If the expression was defined incorrectly (for example, an opening parenthesis was not matched with a closing parenthesis), you receive an error message.

6. Click **OK** to close the **Add Complex Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Devices dialog box.

Oracle IRM Content Groups

Oracle IRM groups are used to control access to documents that have been sealed using Oracle Information Rights Management (IRM). By defining rules based on Oracle IRM groups, you can selectively allow or deny access to IRM-protected documents depending on the contexts that these documents are sealed to. For detailed information on Oracle IRM and how it protects documents, refer to the Oracle documentation.

By defining rules based on Oracle IRM groups, you can, for example, allow certain users or groups to write files sealed to the "Planning" context to Removable devices. You can prevent certain users or groups from writing documents containing more than 5 credit card numbers to Removable devices but allow them to write documents sealed to the "Customer Data" context to Removable devices.

Before defining rules based on Oracle IRM groups, configure DeviceLock Service for Oracle IRM support in **Service Options**.

There are no predefined (built-in) Oracle IRM content groups to use. The following procedure describes how to create your own Oracle IRM group.

To create an Oracle IRM group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Service Settings Editor, do the following:

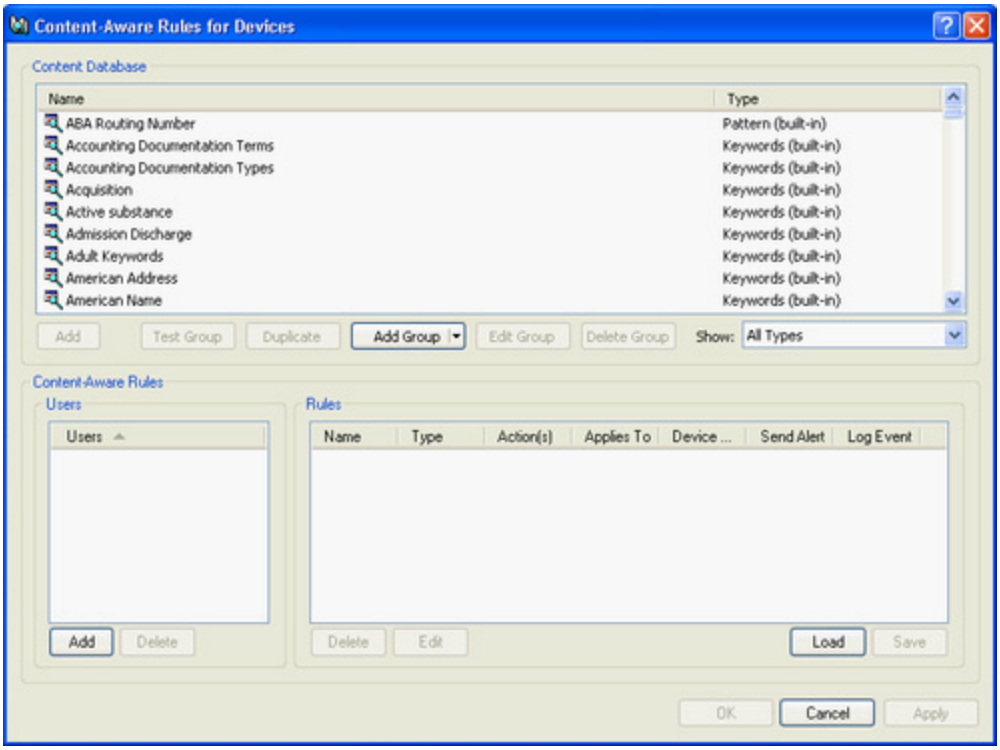
a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

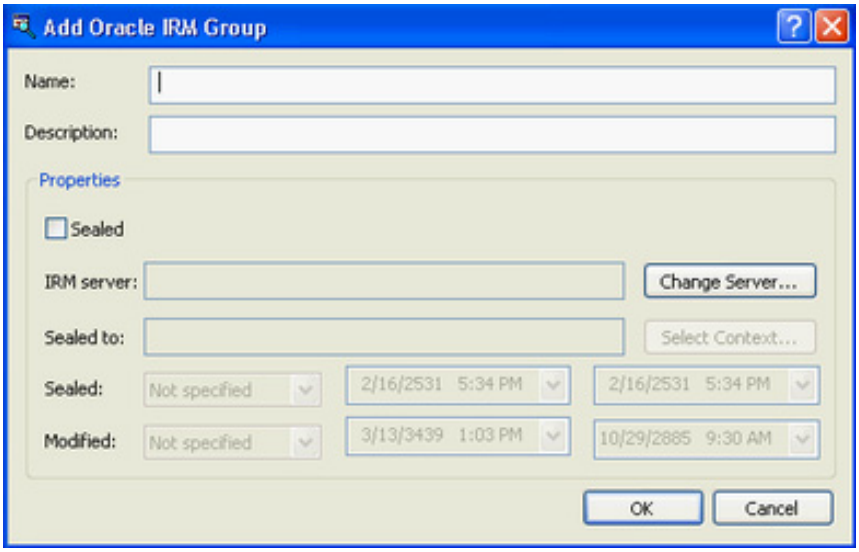
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

The Content-Aware Rules for Devices dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Oracle IRM**.

   The Add Oracle IRM Group dialog box appears.



5. In the **Add Oracle IRM Group** dialog box, do the following:

USE THIS	TO DO THIS
Name	Specify the name of the group.
Description:	Specify a description for the group.
Sealed	Detect and control access to documents that have been sealed using IRM. If you select the **Sealed** check box for an Oracle IRM group and then create a Content-Aware Rule based on this content group, this rule will control access to sealed documents.
IRM Server: Change Server	Specify or change the Oracle IRM server settings supported by DeviceLock Service. To do so, click **Change Server** to open the **Oracle IRM Server Settings** dialog box. In the **Oracle IRM Server Settings** dialog box, do the following: 1. In the **Server URL** box, specify the URL of the IRM server used to seal documents for which you want to control access. To remove the specified IRM server, click **Remove**. 2. In the **User name** box, specify the user account to use for authentication with the IRM server. 3. In the **Password** box, specify the password corresponding to the user account to use for authentication with the IRM server. 4. Click **Validate** to contact the specified IRM server and validate the URL against the one configured on the IRM Server. 5. Click **OK**.
Sealed to	Select the context(s) for which you want to control access. To do so, click **Select Context** to open the **Available contexts** dialog box. In the **Available contexts** dialog box, select the desired context, and then click **OK**. *To update the list of contexts, click Refresh*.

USE THIS	TO DO THIS
	You can select multiple contexts by holding down the SHIFT key or the CTRL key while clicking them. The OR logic is applied to multiple contexts specified within an Oracle IRM group. *You can also type multiple contexts separated by a semicolon (;) directly in the Sealed to box*.
Sealed	Specify the classification date/time of the sealed document. To do so, in the **Sealed** list, click any of the following options: • **Not specified** (this option is selected by default) • **Before than** Indicates that the document's classification date/time must be earlier than the specified date/time. • **After than** Indicates that the document's classification date/time must be later than the specified date/time. • **Between** Indicates that the document's classification date/time must fall within the specified date/time range. • **Not older than** Indicates that the document's classification date/time must not be older than the specified number of seconds, minutes, days, weeks, months, and years. • **Older than** Indicates that the document's classification date/time must be older than the specified number of seconds, minutes, days, weeks, months, and years.
Modified	Specify the last modification date/time of the sealed document. To do so, in the **Modified** list, click any of the following options: • **Not specified** (this option is selected by default) • **Before than** indicates that the file's modified date/time must be earlier than the specified date/time. • **After than** indicates that the file's modified date/time must be later than the specified date/time. • **Between** indicates that the file's modified date/time must fall within the specified date/time range. • **Not older than** indicates that the file's modified date/time must not be older than the specified number of seconds, minutes, days, weeks, months, and years. • **Older than** indicates that the file's modified date/time must be older than the specified number of seconds, minutes, days, weeks, months, and years.

6. Click **OK** to close the **Add Oracle IRM Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Devices dialog box.

Viewing Built-in Content groups

You can view any built-in content groups but you cannot edit or delete them.

To view a built-in content group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Devices dialog box appears.
4. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, select any built-in group you want to view, and then click **View Group**.

Duplicating Built-in Content groups

You cannot edit the built-in content groups but you can create and use their editable copies (duplicates) to suit your particular organization's needs.

To duplicate a built-in content group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Devices dialog box appears.
4. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, select any built-in group you want to duplicate, and then click **Duplicate**.
5. In the dialog box that opens, edit the content group as required, and then click **OK**.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Devices dialog box.

Editing and Deleting Custom Content Groups

You can modify or delete custom content groups at any time.

To edit or delete a custom content group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Devices dialog box appears.
4. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, select any custom group you want to edit or delete.
5. Click **Edit Group** to modify the selected content group. In the dialog box that opens, make the required changes, and then click **OK**.

   - OR -

   Click **Delete Group** or press the DELETE key to delete the selected content group.

6. In the **Content-Aware Rules for Devices** dialog box, click **OK** or **Apply** to apply the changes.

Testing Content Groups

You can test any built-in or custom content group to see whether specified files match with it. By using these tests, you can verify that the rules that are created based on the content groups meet your specific business requirements.

To test a content group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Devices dialog box appears.
4. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, select any content group you want to test, and then click **Test Group**.

   You can test only one group at a time.

   The Open dialog box appears.
5. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to use for testing the specified content group.
6. In the folder list, locate and open the folder that contains the file.
7. Click the file, and then click **Open**.

   The Result message box is displayed. If the file matches with the specified content group, the Result message box contains the following text: "Selected file matches with the group." If the file does not match with the specified content group, the Result message box contains the following text: "Selected file does not match with the group."

The maximum allowable file size is 5 MB. If your file exceeds 5 MB, you may receive the following error message: "File too large." This restriction applies only to DeviceLock WebConsole.

When testing is in progress, the console stops responding (hangs)

Managing Content-Aware Rules

Managing Content-Aware Rules involves the following tasks:

- Defining Content-Aware Rules
- Editing Content-Aware Rules
- Copying Content-Aware Rules
- Exporting and importing Content-Aware Rules
- Undefining Content-Aware Rules
- Deleting Content-Aware Rules

You can manage Content-Aware Rules using DeviceLock Management Console, DeviceLock Group Policy Manager, or DeviceLock Service Settings Editor.

Defining Content-Aware Rules

Content-Aware Rules are created based on either the built-in or custom content groups. For detailed information on these groups, see "Configuring Content Detection Settings."

You can enable alerts that are sent when a specific Content-Aware Rule fires. Such alerts are enabled at the time you define a Content-Aware Rule.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific Content-Aware Rule, you must configure alert settings in **Service Options**.

To define a Content-Aware Rule

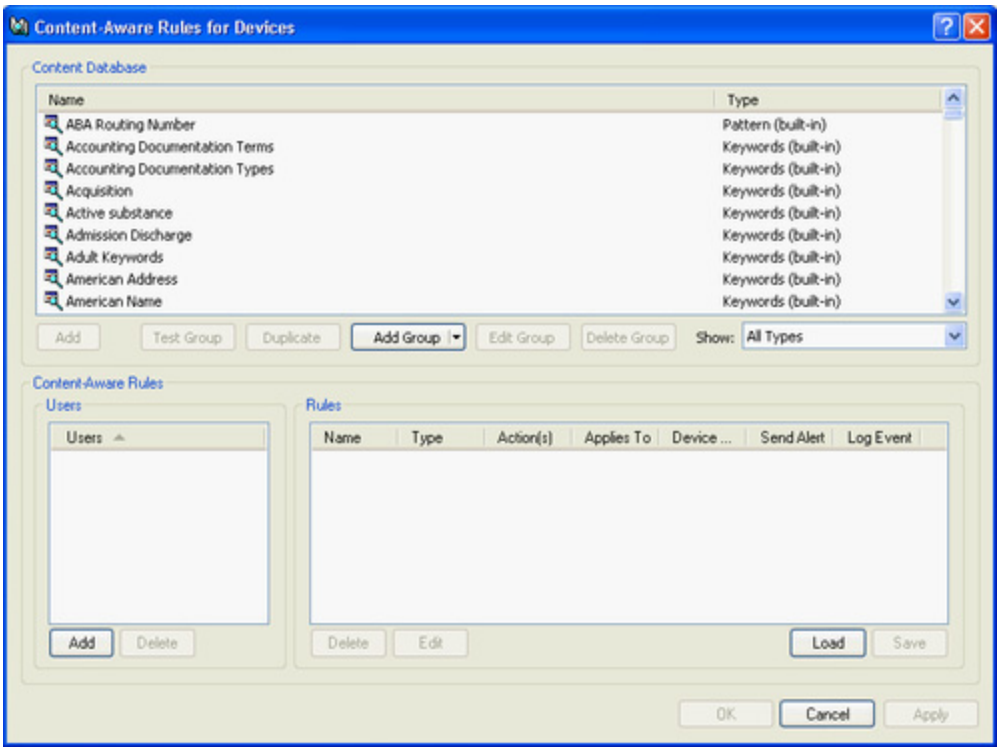
1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.

3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Devices dialog box appears.



4. In the lower-left pane of the **Content-Aware Rules for Devices** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Devices dialog box.

   To delete a user or group, in the lower-left pane of the **Content-Aware Rules for Devices** dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

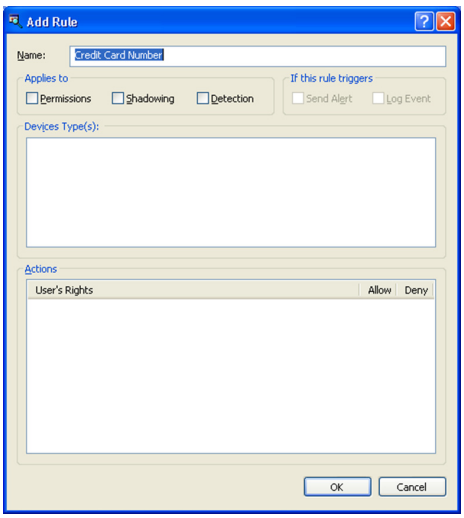
6. In the lower-left pane of the **Content-Aware Rules for Devices** dialog box, under **Users**, select the users or groups for which you want to define the rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

7. In the upper pane of the **Content-Aware Rules for Devices** dialog box, under **Content Database**, select the desired content group, and then click **Add**.

   Note: You can specify only one content group for a Content-Aware Rule.

   The Add Rule dialog box appears.



8. In the **Add Rule** dialog box, in the **Name** box, type the name of the Content-Aware Rule.

   By default, the Content-Aware Rule has the same name as the specified content group but you can enter a different name.

9. Under **Applies to**, specify the type of operation associated with the rule. The available options are:

   - **Permissions**: Specifies that the rule will apply to access control operations.
   - **Shadowing**: Specifies that the rule will apply to shadow copy operations.
   - **Detection**: Specifies that the rule will detect specified content in transferred data, log detection events, and send alerts to the administrator if the appropriate flags have been set.
   - **Permissions**, **Shadowing**: Specifies that the rule will apply to both access control and shadow copy operations.
   - **Permissions, Detection**: Specifies that the rule will apply to both access control and detection operations.
   - **Shadowing, Detection**: Specifies that the rule will apply to both shadow copy and detection operations.
   - **Permissions, Shadowing, Detection**: Specifies that the rule will apply to both access control and shadow copy operations, as well as to detection operations.

10. Under **If this rule triggers**, specify the following additional actions to be performed when the rule triggers:

    - **Send Alert**: Specifies that an alert is sent whenever the rule triggers.
    - **Log Event**: Specifies that an event is logged in the Audit Log whenever the rule triggers.

Note: Alerts and audit enabled for Content-Aware Rules have a priority over device type-specific alerts and audit. For example, if you enable alerts and audit for a specific device type and do not enable alerts and audit for a Content-Aware Rule associated with the same device type, DeviceLock will not send an alert and will not log an event when the rule fires. For another example, if you enable alerts and audit for a Content-Aware Rule associated with a specific device type and do not enable alerts and audit for the same device type, DeviceLock will send an alert and log an event when the rule fires.

11. Under **Device Type(s)**, select the appropriate device type(s) you would like this rule to be applied to.

    Content-Aware Rules can be applied to the following device types: Clipboard, Floppy, iPhone, MTP, Optical Drive, Palm, Printer, Removable, TS Devices, and Windows Mobile.

    Under Action(s), if you multi-select device types that have different combinations of configurable access rights, the dialog box will display the superset of access rights for the selection list: those that are common to all selected device types, and those that do not necessarily apply to all types. As would be expected, if a particular access right that is displayed is not common to one or more particular selected device types, it's setting will not/cannot be applied to those device types and will only apply to types where the setting is supported.

12. Under **Action(s)**, specify which user actions are allowed or disallowed on files, which user actions are logged to the Shadow Log, and which user actions are detected.

    You can select any of the following options: Read, Write, Read and Write.

    If the rule applies to shadow copy operations combined with other operations, the Read user right becomes unavailable. If the rule applies to detection operations combined with other operations, only Allow action becomes available. For detailed information on user rights and actions that can be specified in Content-Aware Rules, see "Content-Aware Rules for Access Control Operations", "Content-Aware Rules for Shadow Copy Operations" and "Content-Aware Rules for Detection Operations".

13. Click **OK**.

    The rule you created is displayed under Rules in the lower-right pane of the Content-Aware Rules dialog box.

14. Click **OK** or **Apply** to apply the rule.

    The users or groups to which the Content-Aware Rule applies are displayed under Content-Aware Rules in the console tree. When you select a user or group to which a Content-Aware Rule applies in the console tree, in the details pane you can view detailed information regarding this rule. This information includes the following:

    - **Name** The name of the rule. By default, the rule has the same name as the specified content group.
    - **Type** The type of the content analysis. Possible values: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties**, **Complex** and **Oracle IRM**. **File Type Detection** indicates that recognition and identification of files is based on their characteristic signatures. **Keywords** indicates that recognition and identification of data/files is based on the specified keywords or phrases. **Pattern** indicates that recognition and identification of data/files is based on the specified patterns of text described by Perl regular expressions. **Document Properties** indicates that recognition and identification of files is

based on their properties. **Complex** indicates that recognition and identification of data/files is based on the specified content described by a Boolean expression. **Oracle IRM** indicates that recognition and identification of files is based on their IRM contexts.

- **Action(s)** Shows which user actions are allowed or disallowed on files and which user actions are logged to the Shadow Log.
- **Applies To** Possible values: **Permissions**, **Shadowing**, **Detection**, **Permissions+Shadowing**, **Permissions+Detection, Shadowing+Detection, Permissions+Shadowing+Detection** **Permissions** indicates that the rule applies to access control operations. **Shadowing** indicates that the rule applies to shadow copy operations. **Detection** indicates that the rule applies to detection operations. **Permissions+Shadowing** indicates that the rule applies to both access control and shadow copy operations. **Permissions+Detection** indicates that the rule applies to both access control and detection operations. **Shadowing+Detection** indicates that the rule applies to both shadow copy and detection operations. **Permissions+Shadowing+Detection** indicates that the rule applies to all available operations: access control, shadow copy and detection.
- **Device Type(s)** The device type(s) to which the rule applies.
- **Send Alert** Shows whether alerts are enabled or disabled for this rule.
- **Log Event** Shows whether audit logging of events associated with this rule is enabled or disabled.
- **Profile** Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to computers that are working offline.

  You can define different online vs. offline Content-Aware Rules for the same user or sets of users. For information about how to define offline Content-Aware Rules, see "Managing Offline Content-Aware Rules for Devices."

Editing Content-Aware Rules

You can modify the Content-Aware Rule properties such as **Name**, **Applies To**, **If this rule triggers**, **Device Type(s)**, **Actions**.

To edit a Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.

3. Under **Devices**, right-click **Content-Aware Rules**, click **Manage**, and then do the following:

    a) In the lower-left pane of the **Content-Aware Rules for Devices** dialog box, under **Users**, select the user or group for which you want to edit the rule.

    By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.

    b) In the lower-right pane of the **Content-Aware Rules for Devices** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.

    - OR -

    Right-click the rule, and then click **Edit**.

    - OR -

    Under **Devices**, expand **Content-Aware Rules**, and then do the following:

    a) Under **Content-Aware Rules**, select the user or group for which you want to edit the rule.

    By selecting users or groups, you can view the Content-Aware Rules applied to them in the details pane.

    b) In the details pane, right-click the rule you want to edit, and then click **Edit**.

    - OR -

    In the details pane, double-click the rule you want to edit.

    The Edit Rule dialog box appears.

4. In the **Edit Rule** dialog box, modify the rule properties as required to meet your needs.
5. Click **OK** to apply the changes.

Copying Content-Aware Rules

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing Content-Aware Rules.

To copy a Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:

    a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
    b) In the console tree, expand **DeviceLock Service**.

    If you use DeviceLock Service Settings Editor, do the following:

    a) Open DeviceLock Service Settings Editor.
    b) In the console tree, expand **DeviceLock Service**.

    If you use DeviceLock Group Policy Manager, do the following:

    a) Open Group Policy Object Editor.
    b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, do one of the following:

- Right-click **Content-Aware Rules**, and then click **Manage**.
  - OR -
- Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

The Content-Aware Rules for Devices dialog box appears.

4. In the lower-left pane of the **Content-Aware Rules for Devices** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.

   By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.

5. In the lower-right pane of the **Content-Aware Rules for Devices** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

   The rule you cut or copy is automatically copied to the Clipboard.

   You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.

   To perform a drag-and-drop operation, select the rule and move it to the user or group to which you want to apply the copied rule.

6. In the lower-left pane of the **Content-Aware Rules for Devices** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Devices dialog box.

8. In the lower-left pane of the **Content-Aware Rules for Devices** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

9. In the lower-right pane of the **Content-Aware Rules for Devices** dialog box, right-click in the **Rules** pane and then click **Paste**.

   The copied rule is displayed under Rules in the lower-right pane of the Content-Aware Rules for Devices dialog box.

10. Click **OK** or **Apply** to apply the copied rule.

Exporting and Importing Content-Aware Rules

You can export all your current Content-Aware Rules to a .cwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

To export Content-Aware Rules

1. If you use DeviceLock Management Console, do the following:

a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Save**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Save** on the toolbar.
     - OR -
   - Expand **Content-Aware Rules**, right-click any user or group to which the rule is applied, and then click **Save**.
     - OR -
   - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Save**.
     - OR -
   - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Save** on the toolbar.
     - OR -
   - Right-click **Content-Aware Rule**s, and then click **Manage**. In the lower-right pane of the **Content-Aware Rules for Devices** dialog box, under **Rules**, click **Save**.

   The Save As dialog box appears.
4. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the .cwl file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.

   When you export rules, they are saved in a file with a .cwl extension.

To import Content-Aware Rules

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Load**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Load** on the toolbar.
     - OR -
   - Expand **Content-Aware Rules**, right-click any user or group to which the rule is applied, and then click **Load**.
     - OR -
   - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Load**.
     - OR -
   - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Load** on the toolbar.
     - OR -
   - Right-click **Content-Aware Rules**, and then click **Manage**. In the lower-right pane of the **Content-Aware Rules for Devices** dialog box, under **Rules**, click **Load**.

   The Open dialog box appears.
4. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
5. In the folder list, locate and open the folder that contains the file.
6. Click the file, and then click **Open**.

   You can import only one .cwl file at a time.

Undefining Content-Aware Rules

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent Content-Aware Rules from being applied to a specific group of client computers. To do so, you need to return the previously defined Content-Aware Rules to the unconfigured state. All undefined DeviceLock settings are ignored by client computers.

To undefine Content-Aware Rules

1. If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.

b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined DeviceLock policies.
c) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, right-click **Content-Aware Rules**, and then click **Undefine**.

Deleting Content-Aware Rules

You can delete individual Content-Aware Rules when they are no longer required.

To delete a Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:

a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, do one of the following:

- Expand **Content-Aware Rules**, right-click the user or group to which the rule is applied, and then click **Delete user**.
  When you delete a user or group, the rule associated with this user or group is automatically deleted.

  - OR -
- Expand **Content-Aware Rules**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.
  - OR -
- Right-click **Content-Aware Rules**, and then click **Manage**. In the lower-left pane of the **Content-Aware Rules for Devices** dialog box, under **Users**, select the user or group to which the rule is applied. In the lower-right pane of the **Content-Aware Rules for Devices** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.
  You can select multiple rules that you want to delete by holding down the SHIFT key or the CTRL key while clicking them.

Content-Aware Rules for Protocols (Regular Profile)

Content-Aware Rules extend the protocol access control functionality of DeviceLock DLP Suite by adding comprehensive, content-level protection of corporate data containing confidential company information. Content-Aware Rules enable automatic content inspection of data/files transmitted over the network, detection of sensitive content and enforcement of regulatory policies to ensure protection.

With Content-Aware Rules, you can selectively allow or deny access to specific content transmitted over the network regardless of preset permissions at the protocol – level. You can also use Content-Aware Rules to allow or deny shadow copying of specific content, or to detect user attempts to transfer specific content over a protocol, without blocking/delaying transfer or creating shadow copies. For flexibility, Content-Aware Rules can be defined on a per-user or per-group basis.

You can configure Content-Aware Rules to apply to access control operations, to shadow copy operations, to detection operations, or to all of the above.

The following examples illustrate the use of Content-Aware Rules.

- **Example 1 – Using Content-Aware Rules for access control operations**. You can prevent certain users or groups from uploading files containing credit card numbers, telephone numbers and addresses to an FTP server.
- **Example 2 – Using Content-Aware Rules for shadow copy operations**. You can specify that IM conversations containing credit card numbers and e-mail addresses will be shadow copied for security auditing and incident investigation purposes.
- **Example 3 – Using Content-Aware Rules for detection operations.** You can specify that only attempts to transfer executable files will be logged and alerted on, without blocking/delaying the transfer or creating shadow copies.

Note: You can define different online vs. offline Content-Aware Rules for the same user or sets of users. Online Content-Aware Rules (Regular Profile) apply to client computers that are working online. Offline Content-Aware Rules (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define offline Content-Aware Rules for protocols, see "Managing Offline Content-Aware Rules for Protocols."

Content-Aware Rules for Access Control Operations

Content-Aware Rules allow you to do the following:

- Grant access to specified content when access is denied at the protocol-level.
- Deny access to specified content when access is granted at the protocol-level.

Content-Aware Rules also override any rules defined in the Protocols White List.

The following table provides summary information on access rights that can be specified for each protocol in Content-Aware Rules.

PROTOCOL	ACCESS RIGHTS	DESCRIPTION
FTP	Generic: Outgoing Files	Controls whether the user can upload files with specified content to an FTP server.
	SSL: Outgoing Files	Controls whether the user can upload files with specified content to an FTP server using FTPS.
HTTP, File Sharing	Generic: POST Requests	Controls whether the user can submit Web form data with specified content to a Web server using HTTP.
	Generic: Outgoing Files	Controls whether the user can upload files with specified content to a Web server using HTTP.
	SSL: POST Requests	Controls whether the user can submit Web form data with specified content to a Web server using HTTPS.
	SSL: Outgoing Files	Controls whether the user can upload files with specified content to a Web server using HTTPS.
IBM Notes	Generic: Outgoing Messages	Controls whether the user can send e-mail messages with specified content from the IBM Notes client to IBM Domino server.
	Generic: Outgoing Files	Controls whether the user can send e-mail attachments with specified content from the IBM Notes client to IBM Domino server.
ICQ/AOL Messenger, IRC	Generic: Outgoing Messages	Controls whether the user can send instant messages with specified content.
	Generic: Outgoing Files	Controls whether the user can send files with specified content.
	SSL: Outgoing Messages	Controls whether the user can send instant messages with specified content using SSL.
	SSL: Outgoing Files	Controls whether the user can send files with specified content using SSL.
Mail.ru Agent, Jabber, Skype, Windows Messenger, Yahoo Messenger	Generic: Outgoing Messages	Controls whether the user can send instant messages with specified content.
	Generic: Outgoing Files	Controls whether the user can send files with specified content.
MAPI	Generic: Outgoing Messages	Controls whether the user can send e-mail messages with specified content from the Outlook client to Microsoft Exchange Server.

	Generic: Outgoing Files	Controls whether the user can send e-mail attachments with specified content from the Outlook client to Microsoft Exchange Server.
SMTP, Web Mail	Generic: Outgoing Messages	Controls whether the user can send e-mail messages with specified content.
	Generic: Outgoing Files	Controls whether the user can send e-mail attachments with specified content.
	SSL: Outgoing Messages	Controls whether the user can send e-mail messages with specified content using SSL.
	SSL: Outgoing Files	Controls whether the user can send e-mail attachments with specified content using SSL.
Social Networks	Generic: Outgoing Messages	Controls whether the user can send messages, comments, and posts with specified content.
	Generic: Outgoing Files	Controls whether the user can send media and other files with specified content to a social networking site.

Note: If the No Access permission is set for a protocol and there is a Content-Aware Rule that allows access to specified content for the same protocol, the Send/Receive Data access right is automatically granted to users for this protocol. For more information about this access right, see "Managing Permissions for Protocols."

The **POST Requests** access right for the **File sharing** protocol, when applied to the iCloud service, controls whether a user can upload non-file data (Mail, Notes, Calendar, Contacts, Reminders) to iCloud. The same access right enables audit logging and shadow copying of the non-file data uploaded to iCloud. Audit records of upload attempts and shadow copies of that data are stored as **Outgoing Messages.**

When using Content-Aware Rules, consider the following:

- ***Content-Aware Rules with Deny settings take priority over rules with Allow settings if they apply to the same users or groups. Exception: Content-Aware Rules with Allow settings based on Document Properties group with Text extraction not supported flag enabled take priority over rules with Deny settings and allow transfer any matching content, including split (or multi-volume) archives.***
- ***Content-Aware Rules with Allow settings allow transfer of the whole data object (message or file, including archives and other containers) when the content matches these rules and when the content does not match a Content-Aware Rule with Deny settings.***
- ***Checking the content of files can be a time-consuming operation. You can define a Content verification message to be displayed to users when content inspection is in progress. For detailed information on this message, see "Content verification message" in "Service Options".***
- ***When users try to use protocols to which they are denied access, they receive a Protocols blocked message, if Protocols blocked message is***

enabled in Service Options. For detailed information on this message, see "Protocols blocked message" in "Service Options".

Content-Aware Rules for Shadow Copy Operations

Before you can use Content-Aware Rules for shadow copy operations, you must turn on shadowing in **Auditing, Shadowing and Alerts** at the protocol-level. Content-Aware Rules that apply to shadow copy operations filter the shadow copies of data and files transmitted by the user.

The following table provides summary information on shadowing rights that can be specified for each protocol in Content-Aware Rules.

PROTOCOL	SHADOWING RIGHTS	DESCRIPTION
FTP	Generic: Incoming Files	Controls whether or not files with specified content downloaded from an FTP server are shadow copied.
	Generic: Outgoing Files	Controls whether or not files with specified content uploaded to an FTP server are shadow copied.
	SSL: Incoming Files	Controls whether or not files with specified content downloaded from an FTP server using FTPS are shadow copied.
	SSL: Outgoing Files	Controls whether or not files with specified content uploaded to an FTP server using FTPS are shadow copied.
HTTP, File Sharing	Generic: Incoming Files	Controls whether or not files with specified content downloaded from a Web server are shadow copied.
	Generic: POST Requests	Controls whether or not Web form data with specified content submitted to a Web server is shadow copied.
	Generic: Outgoing Files	Controls whether or not files with specified content uploaded to a Web server are shadow copied.
	SSL: Incoming Files	Controls whether or not files with specified content downloaded from a Web server using HTTPS are shadow copied.
	SSL: POST Requests	Controls whether or not Web form data with specified content submitted to a Web server using HTTPS is shadow copied.
	SSL: Outgoing Files	Controls whether or not files with specified content uploaded to a Web server using HTTPS are shadow copied.
IBM Notes	Generic: Incoming Messages	Controls whether or not e-mail messages with specified content received by the user to the IBM Notes client from IBM Domino server are shadow copied.

PROTOCOL	SHADOWING RIGHTS	DESCRIPTION
	Generic: Incoming Files	Controls whether or not e-mail attachments with specified content received by the user to the IBM Notes client from IBM Domino server are shadow copied.
	Generic: Outgoing Messages	Controls whether or not e-mail messages with specified content sent by the user from the IBM Notes client to IBM Domino server are shadow copied.
	Generic: Outgoing Files	Controls whether or not e-mail attachments with specified content sent by the user from the IBM Notes client to IBM Domino server are shadow copied.
ICQ/AOL Messenger, IRC	Generic: Incoming Messages	Controls whether or not instant messages with specified content received by the user are shadow copied.
	Generic: Incoming Files	Controls whether or not files with specified content received by the user are shadow copied.
	Generic: Outgoing Messages	Controls whether or not instant messages with specified content sent by the user are shadow copied.
	Generic: Outgoing Files	Controls whether or not files with specified content sent by the user are shadow copied.
	SSL: Incoming Messages	Controls whether or not instant messages with specified content received by the user using SSL are shadow copied.
	SSL: Incoming Files	Controls whether or not files with specified content received by the user using SSL are shadow copied.
	SSL: Outgoing Messages	Controls whether or not instant messages with specified content sent by the user using SSL are shadow copied.
	SSL: Outgoing Files	Controls whether or not files with specified content sent by the user using SSL are shadow copied.
Mail.ru Agent, Jabber, Skype, Windows Messenger, Yahoo Messenger	Generic: Incoming Messages	Controls whether or not instant messages with specified content received by the user are shadow copied.
	Generic: Incoming Files	Controls whether or not files with specified content received by the user are shadow copied.
	Generic: Outgoing Messages	Controls whether or not instant messages with specified content sent by the user are shadow copied.
	Generic: Outgoing Files	Controls whether or not files with specified content sent by the user are shadow copied.
MAPI	Generic: Incoming Messages	Controls whether or not e-mail messages with specified content received by the user to the Outlook client from Microsoft Exchange Server are shadow copied.

PROTOCOL	SHADOWING RIGHTS	DESCRIPTION
	Generic: Incoming Files	Controls whether or not e-mail attachments with specified content received by the user to the Outlook client from Microsoft Exchange Server are shadow copied.
	Generic: Outgoing Messages	Controls whether or not e-mail messages with specified content sent by the user from the Outlook client to Microsoft Exchange Server are shadow copied.
	Generic: Outgoing Files	Controls whether or not e-mail attachments with specified content sent by the user from the Outlook client to Microsoft Exchange Server are shadow copied.
SMB	Generic: Incoming Files	Controls whether or not files with specified content downloaded by the user are shadow copied. Also, controls whether or not files with specified content are shadow copied when they are uploaded from external computers to a local shared resource on the computer where DeviceLock Service runs.
	Generic: Outgoing Files	Controls whether or not files with specified content uploaded by the user are shadow copied. Also, controls whether or not files with specified content are shadow copied when they are downloaded to external computers from a local shared resource on the computer where DeviceLock Service runs.
SMTP, Web Mail	Generic: Outgoing Messages	Controls whether or not e-mail messages with specified content sent by the user are shadow copied.
	Generic: Outgoing Files	Controls whether or not e-mail attachments with specified content sent by the user are shadow copied.
	SSL: Outgoing Messages	Controls whether or not e-mail messages with specified content sent by the user using SSL are shadow copied.
	SSL: Outgoing Files	Controls whether or not e-mail attachments with specified content sent by the user using SSL are shadow copied.
Social Networks	Generic: Outgoing Messages	Controls whether or not messages, comments, and posts with specified content sent by the user are shadow copied.
	Generic: Outgoing Files	Controls whether or not media and other files with specified content uploaded to a social networking site are shadow copied.

Note: The **POST Requests** access right for the **File Sharing** protocol, when applied to the iCloud service, enables audit logging and shadow copying of non-file data (Mail, Notes, Calendar, Contacts, Reminders).

Content-Aware Rules for Detection Operations

The following table provides summary information on detection rights that can be specified in Content-Aware Rules.

PROTOCOL	ACCESS RIGHTS	DESCRIPTION
FTP	Generic: Outgoing Files	Controls whether user attempts to upload files with specified content to an FTP server are detected.
	SSL: Outgoing Files	Controls whether user attempts to upload files with specified content to an FTP server using FTPS are detected.
HTTP, File Sharing	Generic: POST Requests	Controls whether user attempts to submit Web form data with specified content to a Web server using HTTP are detected.
	Generic: Outgoing Files	Controls whether user attempts to upload files with specified content to a Web server using HTTP are detected.
	SSL: POST Requests	Controls whether user attempts to submit Web form data with specified content to a Web server using HTTPS are detected.
	SSL: Outgoing Files	Controls whether user attempts to upload files with specified content to a Web server using HTTPS are detected.
IBM Notes	Generic: Outgoing Messages	Controls whether user attempts to send e-mail messages with specified content from the IBM Notes client to IBM Domino server are detected.
	Generic: Outgoing Files	Controls whether user attempts to send e-mail attachments with specified content from the IBM Notes client to IBM Domino server are detected.
ICQ/AOL Messenger, IRC	Generic: Outgoing Messages	Controls whether user attempts to send instant messages with specified content are detected.
	Generic: Outgoing Files	Controls whether user attempts to send files with specified content are detected.
	SSL: Outgoing Messages	Controls whether user attempts to send instant messages with specified content using SSL are detected
	SSL: Outgoing Files	Controls whether user attempts to send files with specified content using SSL are detected.
Mail.ru Agent, Jabber,	Generic: Outgoing Messages	Controls whether user attempts to send instant messages with specified content are detected.

PROTOCOL	ACCESS RIGHTS	DESCRIPTION
Skype, Windows Messenger, Yahoo Messenger	Generic: Outgoing Files	Controls whether user attempts to send files with specified content are detected.
MAPI	Generic: Outgoing Messages	Controls whether user attempts to send e-mail messages with specified content from the Outlook client to Microsoft Exchange Server are detected.
	Generic: Outgoing Files	Controls whether user attempts to send e-mail attachments with specified content from the Outlook client to Microsoft Exchange Server are detected.
SMTP, Web Mail	Generic: Outgoing Messages	Controls whether user attempts to send e-mail messages with specified content are detected.
	Generic: Outgoing Files	Controls whether user attempts to send e-mail attachments with specified content are detected.
	SSL: Outgoing Messages	Controls whether user attempts to send e-mail messages with specified content using SSL are detected.
	SSL: Outgoing Files	Controls whether user attempts to send e-mail attachments with specified content using SSL are detected.
Social Networks	Generic: Outgoing Messages	Controls whether user attempts to send messages, comments, and posts with specified content are detected.
	Generic: Outgoing Files	Controls whether user attempts to send media and other files with specified content to a social networking site are detected.

Configuring Content Detection Settings

Content-Aware Rules are created based on content groups that enable you to centrally define types of content for which you want to control access. Content groups specify content filtering criteria that will be used to select data to which rules should be applied.

All content groups are stored in the Content Database. The same Content Database is used for both devices and protocols. The Content Database is a part of the DeviceLock Service policy and is also saved in an XML file with service settings that can be created using DeviceLock Management Console, DeviceLock Service Settings Editor, and DeviceLock Group Policy Manager.

There are several types of content groups: File Type Detection groups, Keywords groups, Pattern groups, Document Properties groups, Complex groups, and Oracle IRM groups. The sections below describe these groups and how to use them.

File Type Detection Content Groups

File Type Detection groups are used to control access to files based on file types. These groups contain definitions of the file types that make up these groups. A file type definition consists of two properties: a file name extension (for example, DOC) and a description (for example, Microsoft Word document). When you apply a rule based on a File Type Detection group, the rule is applied to all file types included in that group.

DeviceLock includes more than 30 predefined (built-in) File Type Detection groups that you can use to set up the desired configuration of permissions and/or shadow copy operations. You can use the built-in content groups as they are, create their editable copies (duplicates) or create your own content groups to suit your particular organization's needs.

The following table lists these predefined content groups:

BUILT-IN FILE TYPE DETECTION GROUPS	
Android	MS Outlook, Outlook Express & Email archives
Archives	MS PowerPoint
Audio, Video & Flash	MS Project
BlackBerry	MS Publisher
Common Object File Format (COFF)	MS Visio
Database	MS Windows Installer
Executable	MS Windows Memory Dump
Fax Documents	MS Word
FileMaker Pro	MS Works
Fonts	OpenOffice, StarOffice, OpenDocument, etc.
Help Files	Oracle IRM
Images, CAD & Drawing	PDF, PostScript, & XPS Documents
iOS	QuickBooks, Quicken, TurboTax & etc.
Lotus SmartSuite	Rich Text Format
MS Access	Security Certificates
MS Excel	Text, HTML & XML
MS InfoPath	Virtual Machines
MS Money	WordPerfect Office
MS OneNote	

Note: Content-Aware Rules support Word To Go, Sheet To Go, and Slideshow To Go formats for Palm devices. Word To Go format is included in the MS Word and Rich Text Format built-in content groups, Sheet To Go format is included in the MS Excel built-in content group, while Slideshow To Go format is included in the MS PowerPoint built-in content group.

Microsoft Word or Rich Text Format (RTF) files, Excel files and PowerPoint files can be transferred to a Palm device using the Documents To Go application. The Documents To Go application converts these files to special formats: Word and RTF files are converted to Word To Go format, Excel files are converted to Sheet To Go format, while PowerPoint files are converted to Slideshow To Go format. The converted files are automatically downloaded to the Palm when users synchronize.

With built-in content groups, you can quickly create and apply rules without having to define your own content groups.

Note: You can view file type definitions that are included in the built-in File Type Detection groups but you cannot edit or delete them. For information on how to view the built-in content groups, see "Viewing Built-in Content Groups."

Creating Custom File Type Detection Groups

You can define Content-Aware Rules based on your own (custom) content groups if the predefined content groups included with DeviceLock do not meet your requirements. Custom File Type Detection content groups enable you to specify any file types that you want in the same group to better meet your individual business needs.

For example, suppose you need to grant certain users access to Word, Excel, PDF documents and graphic files. To do this, first you create a new File Type Detection content group that represents these document content types. Then you define a rule based on this custom content group.

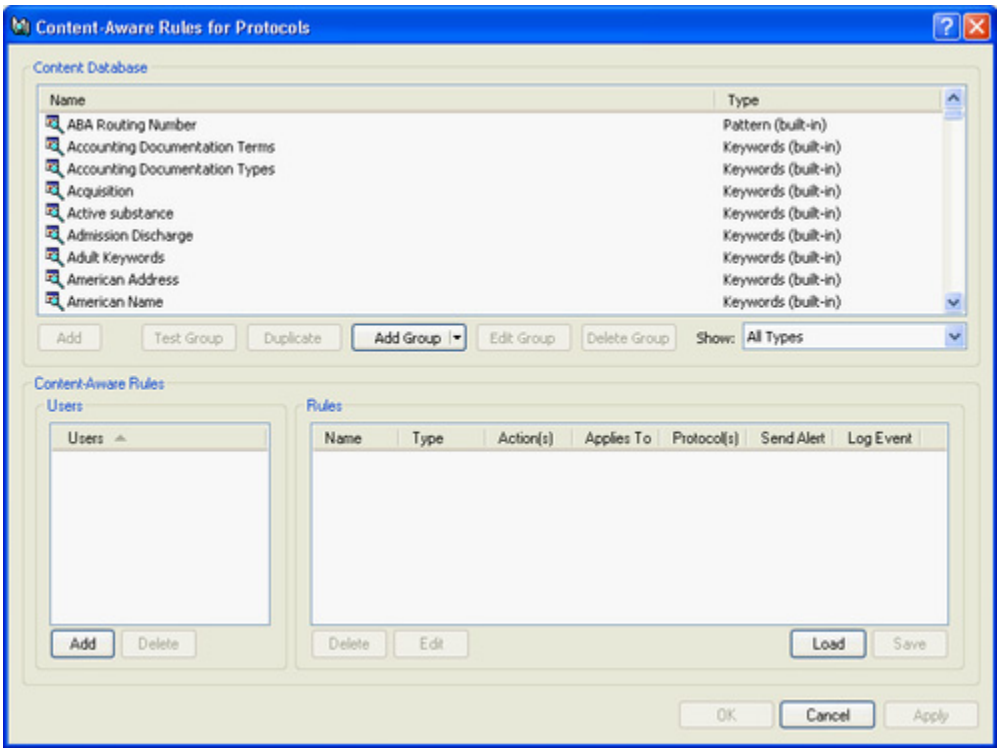
To create a custom File Type Detection group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

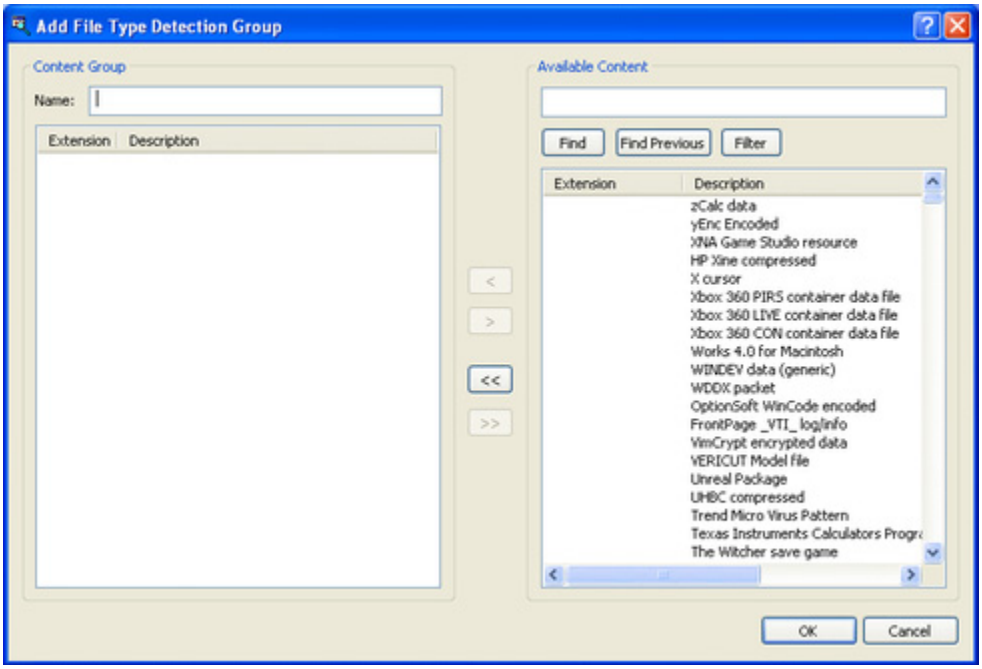
   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Protocols dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **File Type Detection**.

   The Add File Type Detection Group dialog box appears.



5. In the left pane of the **Add File Type Detection Group** dialog box, under **Content group**, type the name of the new content group in the **Name** box.
6. In the right pane of the **Add File Type Detection Group** dialog box, under **Available Content**, select any file type you want to add to the new content group, and then click the left single-arrow button <.

   You can select multiple file types by holding down the SHIFT key or the CTRL key while clicking them.

   To remove single file types from the content group, use the right single-arrow button >. To add or remove all available file types to or from the content group at the same time, use the left double-arrow button << or right double-arrow button >>.

   Note: You can search the available content database for specific file types by extension or description. You can use wildcards such as asterisks (*) and question marks (?) to search for a specific group of file types. To find a specific file type or specific group of file types, under **Available Content**, type an extension or description with or without wildcards in the search string, and then click **Find**. To filter file types, click **Filter**. To remove the filter, apply it to an empty string.

   An asterisk (*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity.
7. Click **OK** to close the **Add File Type Detection Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Protocols dialog box.

Keywords Content Groups

Keywords groups are used to control access to data/files based on specified keywords or phrases.

DeviceLock includes more than 160 predefined (built-in) Keywords groups that you can use to set up the desired configuration of permissions and/or shadow copy operations. You can use the built-in content groups as they are, create their editable copies (duplicates) or create your own content groups to suit your particular organization's needs.

The following table lists these predefined content groups:

BUILT-IN KEYWORDS GROUPS	
Accounting Documentation Terms	Production Charges
Accounting Documentation Types	Profanity
Acquisition	Profiles
Active substance	Profit Loss
Admission Discharge	Project Names
Adult Keywords	Project Release Dates
American Address	Property
American Name	Racism Keywords
Bank ABA	Resume
Bank ACNT	Russian: Account Statement
Bank STMT	Russian: Accounting Documentation

BUILT-IN KEYWORDS GROUPS

Board Meeting	Russian: Accounting Documentation Terms
Breach of Obligation	Russian: Accounting Documentation Types
Breach of Standards	Russian: Bank Account
Breach of the Law	Russian: Bank Operations
Business Documentation	Russian: Banking Operations Participants
Business Documentation Terms	Russian: Breach of Commitment
Business Documentation Types	Russian: Breach of Law
Business Rivals	Russian: Business Documentation
Business Trips & Meetings	Russian: Business Documentation Terms
C# Source Code	Russian: Business Documentation Types
C/C++ Source Code	Russian: Business Partners
Cellular Operator Call Log	Russian: Business Trips & Meetings
COBOL Source Code	Russian: Company Development Plan
Common Disease	Russian: Compensation and Benefits
Common Medical Terms	Russian: Confidential Information
Company Development	Russian: Corporate Capital
Compensation and Benefits	Russian: Corporate Property
Compliance Report	Russian: Expenses
Confidential	Russian: Failures
Confidential Partners Information	Russian: Financial Information
Credit Report	Russian: Financial Report
Credits	Russian: Financial Terms
Discontent	Russian: Firing
Discrediting Information	Russian: Innovations
Driver's License	Russian: Insurance
Employer Identification Number	Russian: Internal Payments
Ethnicity	Russian: Investors and Investments
Executive Job Searches	Russian: Labor Law
Failures	Russian: Loans and Credits
Financial Report	Russian: Manufacturing
Financial Statements	Price List
Firing	Prices
FITS Date & Time	Pro Earnings
FITS File Checksum	Russian: Market Development Plan
FITS File Descriptors	Russian: Medicinal Active Substances
FITS Hierarchical file grouping	Russian: Medicinal Drugs
FITS Instrumentorum	Russian: Noncompliant
FITS Non-standard	Russian: Passwords and Access Codes
FITS Observations	Russian: Physical Security
FITS Standard	Russian: Prices
Gambling	Russian: Project Documentation
Grades	Russian: Project Names
HCFA (CMS) 1500 Form	Russian: Project Versions
HIPAA - Diseases	Russian: Projects Release Date
HIPAA HCPCS	Russian: Technology
HIPAA ICD 10 - Diseases and Injuries	Russian: User Names
HIPAA ICD 10 - Drugs and Chemicals	Russian: Working Conditions
HIPAA ICD9	Sales Forecast
HIPAA NDC Classes	Sarbanes-Oxley Sensitive
HIPAA NDC Dosages	Security
HIPAA NDC Listing	Security Agencies
HIPAA NDC Routes	Sensitive Disease
Illegal Drugs	Sexual Language
Innovations	Social Security
Internet Slang Abbreviations	SPAM
Investments	Sports

BUILT-IN KEYWORDS GROUPS	
Java Source Code	Staff Training
Japan: Surname in Hiragana	Substance Abuse
Japan: Surname in Kanji	Suspicious Activity Report
Japan: Surname in Katakana	Technology
Japan: Surname in One-Byte-Katakana	UBO4 Form
Market Development	US Birth Date
Medical Diagnosis	US Birth Place
Medical Record Numbers	US Expiry Date
MEMO	User Name
Network Security	VB Source Code
Partner Names	Violence
Password	Weapon Keywords
Payments	Wire Transfer
PCI GLBA	Working Conditions
Perl Source Code	

With built-in content groups, you can quickly create and apply rules without having to define your own content groups.

Note: You can view keywords that are included in the built-in Keywords groups but you cannot edit or delete them. For information on how to view the built-in content groups, see "Viewing Built-in Content Groups."

Creating Custom Keywords Groups

You can define Content-Aware Rules based on your own (custom) content groups if the predefined content groups included with DeviceLock do not meet your requirements. Custom Keywords content groups enable you to specify any keywords that you want in the same group to better meet your individual business needs.

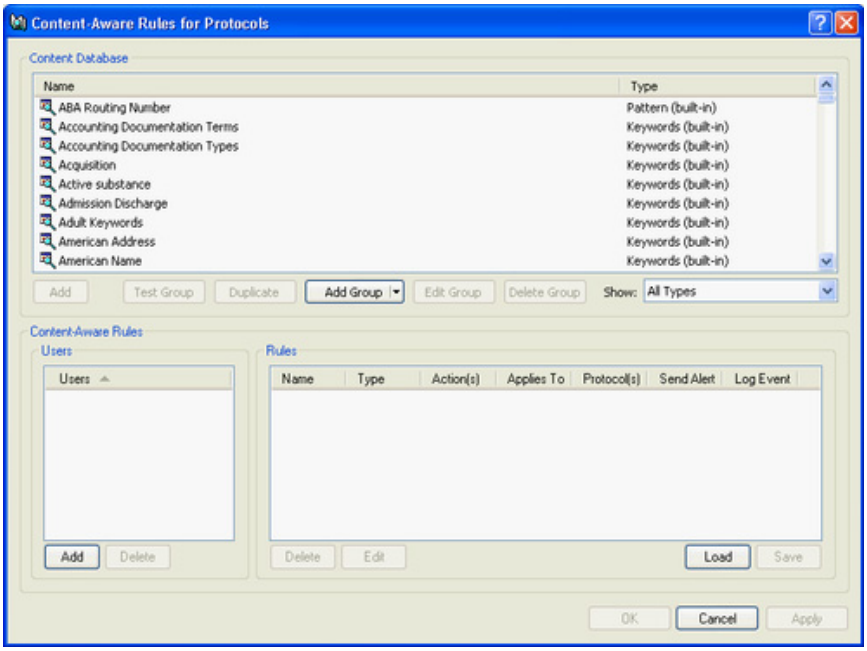
To create a custom Keywords group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

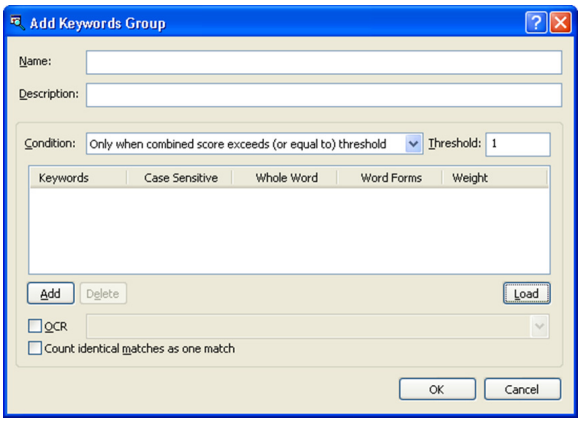
   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

The Content-Aware Rules for Protocols dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Keywords**.

The Add Keywords Group dialog box appears.



5. In the **Add Keywords Group** dialog box, do the following:

USE THIS	TO DO THIS
Name	Specify the name of the group.
Description:	Specify a description for the group.
Condition:	Specify conditions for firing rules associated with this content group. To do so, in the **Condition** list, click any of the following options: • **Match any keyword(s)** indicates that a rule associated with

USE THIS	TO DO THIS
	this content group is activated every time any of the specified keywords is found within text data. • **Match all keyword(s)** indicates that a rule associated with this content group is activated every time all of the specified keywords are found within text data. • **Only when combined score exceeds (or equal to) threshold** indicates that a rule associated with this content group is activated every time the total number (sum) of occurrences of all found keywords within text data equals or exceeds the threshold number of occurrences of the keywords.
Threshold	Specify the threshold number of occurrences of the keywords. This number can range from 0 to 65535. This property requires a value if you selected the **Only when combined score exceeds (or equal to) threshold** option.
Keywords	Specify words and phrases that must occur within text data. Double-click under **Keywords** to enter a keyword or phrase.
Case Sensitive	Determine the case sensitivity of the keywords. Select the **Case Sensitive** check box to specify a case-sensitive comparison of the keywords (for example, the words "test" and "Test" will be treated as different keywords.). Clear the **Case Sensitive** check box to specify a case-insensitive comparison of the keywords (for example, the words "test" and "Test" will be treated as the same keyword).
Whole Word	Specify keyword matching options. Select the **Whole Word** check box to specify the exact match option (allows you to find an exact match of your keyword). Clear the **Whole Word** check box to specify the broad match option (allows you to find all grammatical variations of your keyword).
Word Forms	Specify keyword morphology (linguistics) search options. Select the **Word Forms** check box to enable morphology search for Catalan, English, French, German, Italian, Polish, Portuguese, Russian, and Spanish languages. Also, it enables search support for Russian transliterated words. *The keyword morphology search can be time-consuming and resource-intensive.* Clear the **Word Forms** check box to disable morphology and transliterated search.
Weight	Specify the degree of importance for each keyword or phrase. Weight is used to count the number of occurrences of the specified keywords within text data. This property requires a value if you selected the **Only when combined score exceeds (or equal to) threshold** option. Possible values: **Heavy**, **Above Normal**, **Normal** (default value), **Below Normal**, **Light**. These weight values are interpreted as follows: • **Heavy** weight indicates that each keyword occurrence is

USE THIS	TO DO THIS
	counted as three occurrences. This value is the highest. • **Above Normal** weight indicates that each keyword occurrence is counted as two occurrences. • **Normal** weight indicates that each keyword occurrence is counted as one occurrence. • **Below Normal** weight indicates that two keyword occurrences are counted as one occurrence. • **Light** weight indicates that three keyword occurrences are counted as one occurrence. This value is the lowest.
Add	Specify keywords and phrases. Click **Add** to enter a keyword or phrase.
Delete	Delete a keyword. To do so, select the keyword you want to delete, and then click **Delete**. You can select multiple keywords by holding down the SHIFT key or the CTRL key while clicking them.
Load	Import a list of keywords from a tab-delimited text file.
OCR	Extract text from images for further checking against the list of keywords defined in this content group. To do so, select the **OCR** check box and up to 8 languages. For optimal performance and recognition quality, we recommend that you select only those languages that are really needed.

6. Click **OK** to close the **Add Keywords Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Protocols dialog box.

Pattern Content Groups

Pattern groups let you control access to text data using patterns of text described by Perl regular expressions. Patterns provide a flexible and powerful way to automatically detect potentially sensitive content (for example, credit card numbers, Social Security numbers, e-mail addresses, and phone numbers) within text data.

For more information on creating and using Perl regular expressions, refer to the Perl regular expressions quick start tutorial and Perl regular expressions tutorial.

DeviceLock includes more than 75 predefined (built-in) Pattern groups that you can use to set up the desired configuration of permissions and/or shadow copy operations. You can use the built-in content groups as they are, create their editable copies (duplicates) or create your own content groups to suit your particular organization’s needs.

The following table lists these predefined content groups:

BUILT-IN PATTERN GROUPS

ABA Routing Number	Russian: Classification of Enterprises and Organizations
American Name (Ex)	Russian: Driver's License Number
Austria SSN	Russian: Health Insurance Number
BIC (ISO 9362)	Russian: International Passport
Californian ID Number	Russian: Main State Registration Number
Canadian Postal Code	Russian: Motorcycle Numbers
Canadian Social Insurance Number	Russian: Passport
China National ID	Russian: Pension Insurance Number
Credit Card Number	Russian: Post Code
Danish Personal ID	Russian: Taxpayer Identification Number
Dollar Amount	Russian: Telephone Number
Dominican Republic ID Number	Russian: Trailer Numbers
Email Address	Russian: Vehicle Registration Document
European VAT Number	Scotland CHI
Finnish ID	South African ID Number
France INSEE Code	South Korean Resident Registration Number
French NINO	Spanish DNI
German eTIN	Spanish Full Name
German Telephone Number	Spanish NIF
GPS Data (RMC String)	Spanish SSN
Health Insurance Claim	SQL Queries
IBAN	Sweden Personal ID
International Telephone Number	Sweden Phone Number
IP Address	Sweden Post Code
Irish PPSN	Taiwan: ID Number
Irish VAT	Taiwan: Jih Sun Bank Account Number
ISO Date	TCP/UDP Port Number
Japan: Address	Time (12/24h)
Japan: Date	Turkish ID Number
Japan: Phone Number	UK Date
Japan: Social Security and Tax Number System	UK National Insurance Number
MAC Address	UK NHS Number
Mexican Tax ID Number	UK Phone Number
Microsoft Windows Product Key	UK Post Code
National Provider Identifier	UK RD&E Hospital Number
Norwegian Birth Number	UK Tax Code
Poland National Identity Card Number	Uniform Resource Locator (URL)
Polish ID Number	US Date
RAMQ	US Phone Number
ROK Registration Number	US Social Security Number
Russian: Address	US Zip Code
Russian: Auto Insurance Number	US/UK Home Address
Russian: Bank Account Number	VIN
Russian: BIC	
Russian: Car Numbers	
Russian: Classification of Economic Activities	

With built-in content groups, you can quickly create and apply rules without having to define your own content groups.

Note: You can view regular expression patterns that are included in the built-in Pattern content groups but you cannot edit or delete them. For information on how to view the built-in content groups, see "Viewing Built-in Content Groups."

Creating Custom Pattern Groups

You can define Content-Aware Rules based on your own (custom) content groups if the predefined content groups included with DeviceLock do not meet your requirements. Custom Pattern content groups enable you to specify any pattern that you want to use to identify sensitive information within text data.

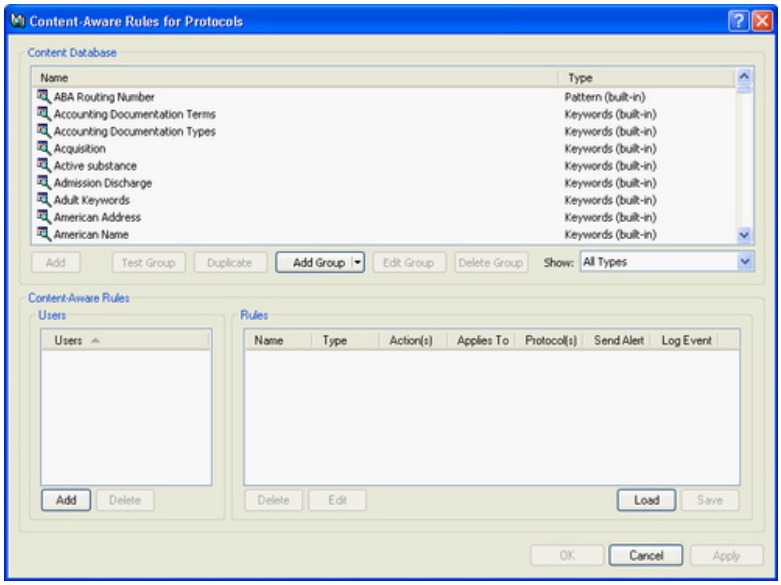
To create a custom Pattern group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

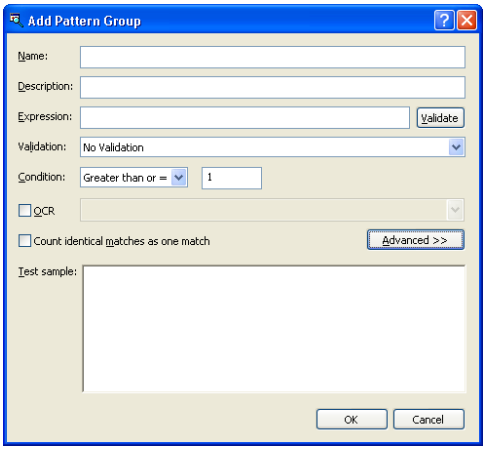
   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Protocols dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Pattern**.

   The Add Pattern Group dialog box appears.



5. In the **Add Pattern Group** dialog box, do the following:

USE THIS	TO DO THIS
Name	Specify the name of the group.
Description:	Specify a description for the group.
Expression	Specify a pattern by creating a regular expression. For information on how to create Perl regular expressions, refer to the Perl regular expressions quick start tutorial and Perl regular expressions tutorial.
Validate	Check regular expression syntax.
Validation	Perform the actual validation on the potential matches returned by the regular expression. The following options are available: **No validation** (this option is selected by default), **ABA Routing Number**, **American Name (Ex)**, **Austria SSN**, **Canadian Social Insurance Number**, **China National ID**, **Credit Card Number (All)**, **Credit Card Number (American Express)**, **Credit Card Number (Diners Club)**, **Credit Card Number (Diners Club En Route)**, **Credit Card Number (Diners Club Carte Blanche)**, **Credit Card Number (Discover)**, **Credit Card Number (JCB)**, **Credit Card Number (Laser)**, **Credit Card Number (Maestro)**, **Credit Card Number (Master Card)**, **Credit Card Number (Solo)**, **Credit Card Number (Switch)**, **Credit Card Number (Visa)**, **Credit Card Number (Visa Electron)**, **Danish Personal ID**, **Date, Date (ISO)**, **Dominican Republic ID**, **Email Address**, **European VAT Number**, **Finnish ID**, **France INSEE Code**, **German eTIN**, **Health Insurance Claim**, **IBAN**, **IP Address**, **Irish PPSN**, **LUHN Checksum**, **Norwegian Birth Number**, **NPI**, **Polish ID**, **Quebec Healthcare Medical Number**, **Mexican Tax Id Number**, **Polish National Identity Card**, **ROK Registration Number**, **Russian Bank Account Number**, **Russian Health Insurance Number**, **Russian Taxpayer Identification Number**, **Russian Main State Registration Number**, **Russian Classification Of Enterprises And Organizations**, **South African Id Number**, **South Korean Resident Registration Number**, **Japan: Social Security and Tax**

USE THIS	TO DO THIS
	Number System, Spanish NIF, Taiwan ID, Turkish Id Number, UK NHS Number, **UK National Insurance Number**, **UK Phone Number**, **UK Post Code**, **UK Tax Code**, **URL**, **US Social Security Number**.
Condition:	Specify conditions for firing rules associated with this content group. To do so, in the **Condition** list, click any of the following options: • **Less than or =** indicates that a rule associated with this content group is activated every time the number of matches returned by the regular expression is less than or equal to the specified number. • **Equal to** indicates that a rule associated with this content group is activated every time the number of matches returned by the regular expression is equal to the specified number. • **Greater than or =** indicates that a rule associated with this content group is activated every time the number of matches returned by the regular expression is greater than or equal to the specified number. • **Between** indicates that a rule associated with this content group is activated every time the number of matches returned by the regular expression is within the specified range.
OCR	Extract text from images for further checking against the regular expression defined in this content group. To do so, select the **OCR** check box and up to 8 languages. For optimal performance and recognition quality, we recommend that you select only those languages that are really needed.
Count identical matches as one match	Combine duplicate matches returned by the regular expression into a single match. To do so, select the **Count identical matches as one match** check box.
Advanced	Quickly test your regular expression pattern on sample data. Click **Advanced** to display or hide the **Test sample** box.
Test sample	Enter a test string and view the result. DeviceLock supports real-time color highlighting of test results. All matches are highlighted in green, while strings that do not match the pattern are highlighted in red.

6. Click **OK** to close the **Add Pattern Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Protocols dialog box.

Document Properties Content Groups

Document Properties groups are used to control access to files based on file properties such as file name, size, etc. You can also use a Document Properties content group to control access to password-protected documents and archives as well as text images.

Note: The AND logic is applied to all file properties specified within a Document Properties group. For example, if you want to control access to files larger than 5 megabyte (MB) in size and password-protected documents and archives, you should create two separate Document Properties groups: one group for files larger than 5 MB in size and another group for password-protected documents and archives. If you specify these file properties within the same Document Properties group and then create a Content-Aware Rule based on this content group, this rule will control password-protected documents and archives that are larger than 5 MB.

There are no predefined (built-in) Document Properties content groups to use. The following procedure describes how to create your own Document Properties group.

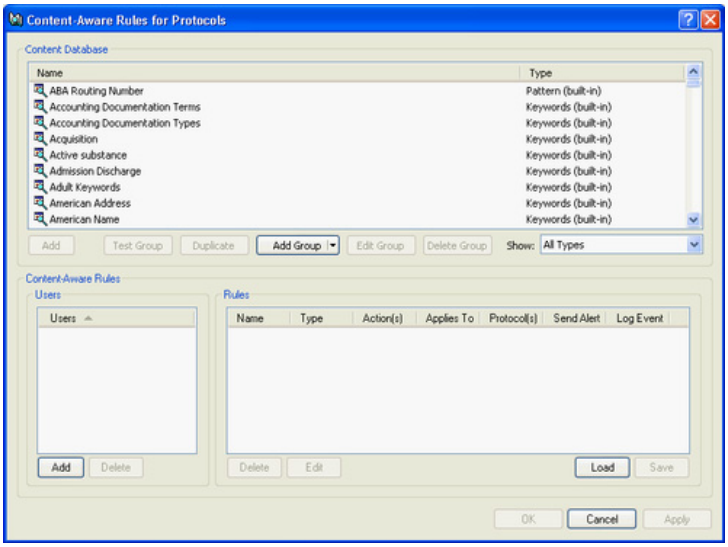
To create a Document Properties group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

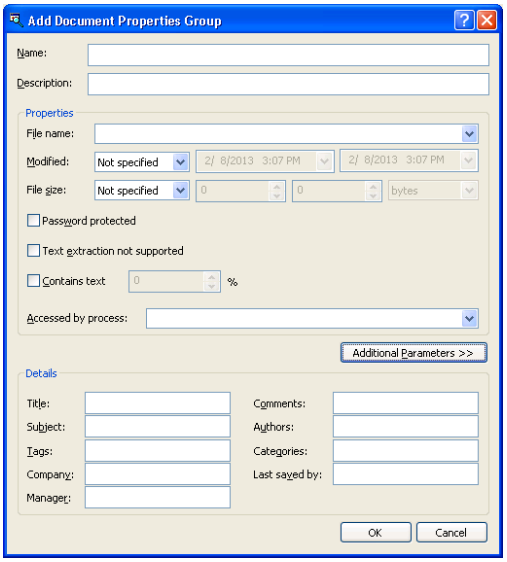
   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Protocols dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Document Properties**.

   The Add Document Properties Group dialog box appears.



5. In the **Add Document Properties Group** dialog box, do the following:

USE THIS	TO DO THIS
Name	Specify the name of the group.
Description:	Specify a description for the group.
File name	Specify the file names. You can use wildcards, such as asterisks (*) and question marks (?). For example, type ***.txt** to specify all files that have the .txt extension. Multiple file names must be separated by a semicolon (;), for example, ***.doc; *.docx**. *An asterisk (*) replaces an unlimited number of characters. The question mark (?) replaces a single character*.
Modified	Specify the last modification date/time of the file. To do so, in the **Modified** list, click any of the following options: • **Not specified** (this option is selected by default) • **Before than** indicates that the file's modified date/time must be earlier than the specified date/time. • **After than** indicates that the file's modified date/time must be later than the specified date/time. • **Between** indicates that the file's modified date/time must fall within the specified date/time range. • **Not older than** indicates that the file's modified date/time must not be older than the specified number of seconds, minutes, days, weeks, months, and years. • **Older than** indicates that the file's modified date/time must be

USE THIS	TO DO THIS
	older than the specified number of seconds, minutes, days, weeks, months, and years. **Note:** The **Modified** property does not apply to files transmitted over the network. If specified, it is ignored during content analysis.
File size	Specify the file size in bytes, kilobytes, megabytes, gigabytes or terabytes. To do so, in the **File size** list, click any of the following options: • **Not specified** (this option is selected by default) • **Equal to** indicates that the file(s) must have a size that is equal to the size you specify. • **Less than** indicates that the file(s) must have a size that is less than the size you specify. • **More than** indicates that the file(s) must have a size that is more than the size you specify. • **Between** indicates that the file size must fall within the specified range.
Password protected	Detect and control access to password-protected archives, PDF files, and Microsoft Office documents (.doc, .xls, .ppt, .docx, .xlsx, .pptx). If you select the **Password protected** check box for a Document Properties group and then create a Content-Aware Rule based on this content group, this rule will control access to password-protected archives, PDF files, and Microsoft Office documents. Clear the **Password protected** check box if you do not want to detect and control access to password-protected archives, PDF files, and Microsoft Office documents. For information on supported archive formats, see the description of the "Inspection of files within archives" feature.
Text extraction not supported	Control access to unsupported file formats. If you select the **Text extraction not supported** check box for a Document Properties group and then create a Content-Aware Rule based on this content group, this rule will control access to all files in an unsupported format. All supported file formats are listed in the "Extending DeviceLock Functionality with ContentLock and NetworkLock" section. You can use this parameter to allow transfer of split (or multi-volume) .cab or .rar archives that by default cannot be unpacked and analyzed in case there are active content-aware rules combined with **Archives content inspection on read** or **Archives content inspection on write** options enabled in **Service options**. Allow Content-Aware Rules based on Document Properties group with **Text extraction not supported** flag enabled take priority over deny rules and allow transfer any matching content, including split (or multi-volume) archives.
Contains text	Detect and control access to images based on whether or not they contain text. If you select the **Contains text** check box for a Document Properties group and then create a complex Content-Aware Rule based on this content group and the built-in Images, CAD & Drawing content group (File Type Detection) combined by the AND operator, this rule will check whether supported image files contain

USE THIS	TO DO THIS
	text and control access to text images. Clear the **Contains text** check box if you do not want to detect and control access to text images. For information on the supported image files, see the description of the "Text in picture detection" feature. If you select the **Contains text** check box, specify the amount of text that images must contain. The amount of text is expressed as a percentage of the total image area. For example, if text occupies ½ of the image, the amount of text makes 50%. If an image contains only text, the amount of text is 100%. **Note:** The **Contains text %** option also applies to other supported file formats. In this case, the percentage means the ratio of the text size in characters to file size in bytes.
Accessed by process	Specify the name of the process accessing the document's file. You can use wildcards, such as asterisks (*) and question marks (?). Multiple process names must be separated by a semicolon (;), for example, **explorer.exe; notepad.exe**.
Additional Parameters	Specify some additional textual parameters supported only for compound documents and new MS Office files (.docx, .xlsx, .pptx). The AND logic is applied to all specified fields. You can use wildcards, such as asterisks (*) and question marks (?). Multiple values must be separated by a semicolon (;), for example, **john; mik***.

6. Click **OK** to close the **Add Document Properties Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Protocols dialog box.

Complex Content Groups

Complex groups use Boolean expressions to select data for which you want to control access. These groups can include any combination of built-in or custom content groups (File Type Detection, Keywords, Pattern, and Document Properties groups) linked with any number of the standard logical operators. Each content group is treated as a single filter criterion that can be included in your Boolean expression. By using multiple content groups, you can create complex filters to identify sensitive content of data transmitted over the network.

The following table lists the logical operators in order of precedence from highest to lowest.

OPERATOR	MEANING
NOT	Logical negation of a filter criterion
AND	Both filter criteria must apply

OPERATOR	MEANING
OR	Either filter criterion can apply

You can use parentheses to modify the precedence of operators and force some parts of an expression to be evaluated before others. Nested criteria enclosed in parentheses are evaluated in inner-to-outer order. Multiple levels of nesting are supported. A complex group can contain a maximum of 50 content groups.

There are no predefined (built-in) Complex content groups to use. The following procedure describes how to create your own Complex group.

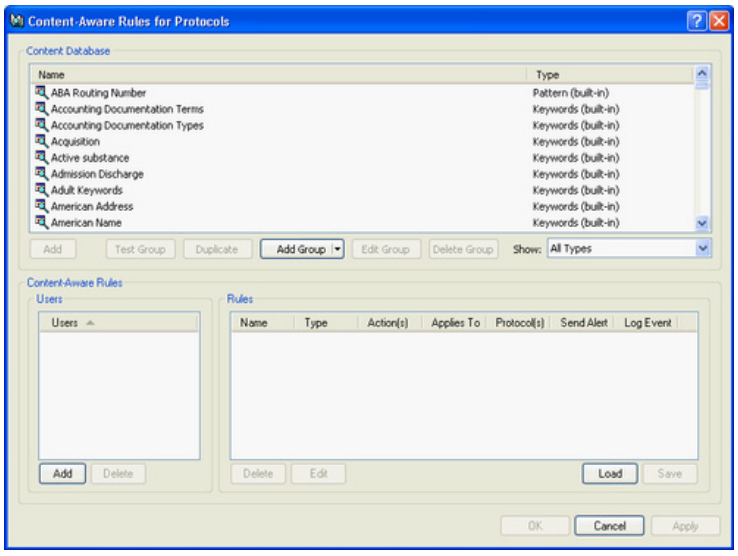
To create a Complex group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

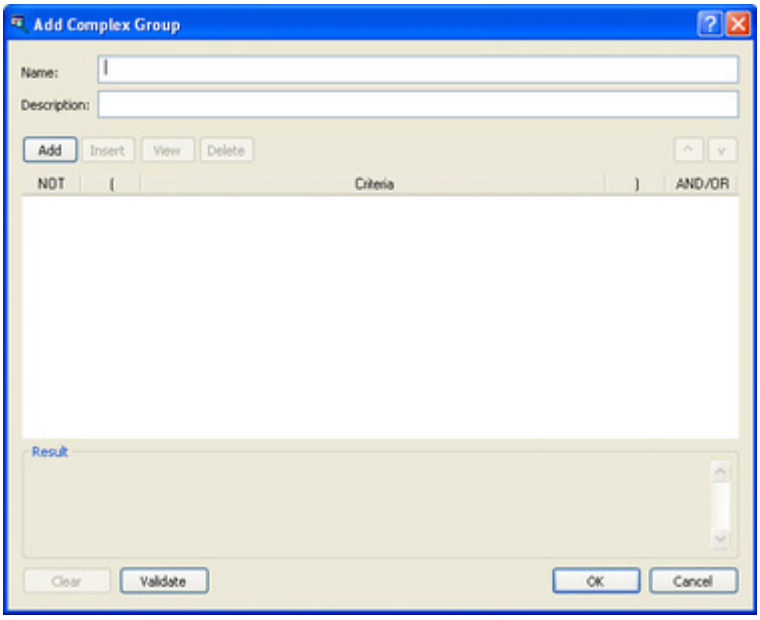
   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Protocols dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Complex**.

   The Add Complex Group dialog box appears.



5. In the **Add Complex Group** dialog box, do the following:

USE THIS	TO DO THIS
Name	Specify the name of the group.
Description:	Specify a description for the group.
Add	Add the desired content groups from the Content Database. To do so, click **Add** to open the **Content Groups** dialog box. In the **Content Groups** dialog box, under **Content Database**, select the desired content group, and then click **OK**. *You can select multiple content groups by holding down the SHIFT key or the CTRL key while clicking them.* *To view information about a content group, select the desired group, and then click View Group*. *The content groups you added appear in the Criteria column in the Add Complex group dialog box. Each content group you add is treated as a single filter criterion that can be included in your Boolean expression*.
Insert	Insert a content group from the Content Database before the currently selected group in the **Criteria** column. To do so, click **Insert** to open the **Content Groups** dialog box. In the **Content Groups** dialog box, under **Content Database**, select the desired content group, and then click **OK**.
View	View information about the currently selected group in the **Criteria** column.

USE THIS	TO DO THIS
Delete	Delete the selected group from the **Criteria** column.
NOT	Join each content group you select with the logical NOT operator. To do so, select the desired group in the **Criteria** column, and then select the appropriate check box in the **Not** column.
AND/OR	Join each content group you select with the logical AND or OR operator. To do so, select the desired group in the **Criteria** column, and then click either **AND** or **OR** in the appropriate list in the **AND/OR** column.
Clear	Clear the current list of content groups in the **Criteria** column.
Validate	Validate your expression. If the expression was defined incorrectly (for example, an opening parenthesis was not matched with a closing parenthesis), you receive an error message.

6. Click **OK** to close the **Add Complex Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Protocols dialog box.

Oracle IRM Content Groups

Oracle IRM groups are used to control access to documents that have been sealed using Oracle Information Rights Management (IRM). By defining rules based on Oracle IRM groups, you can selectively allow or deny access to IRM-protected documents depending on the contexts that these documents are sealed to. For detailed information on Oracle IRM and how it protects documents, refer to the Oracle documentation.

By defining rules based on Oracle IRM groups, you can, for example, allow members of the Researchers group to e-mail documents sealed to the "Internal Research" and "Market Research" contexts using SMTP.

Before defining rules based on Oracle IRM groups, configure DeviceLock Service for Oracle IRM support in **Service Options**.

There are no predefined (built-in) Oracle IRM content groups to use. The following procedure describes how to create your own Oracle IRM group.

To create an Oracle IRM group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.

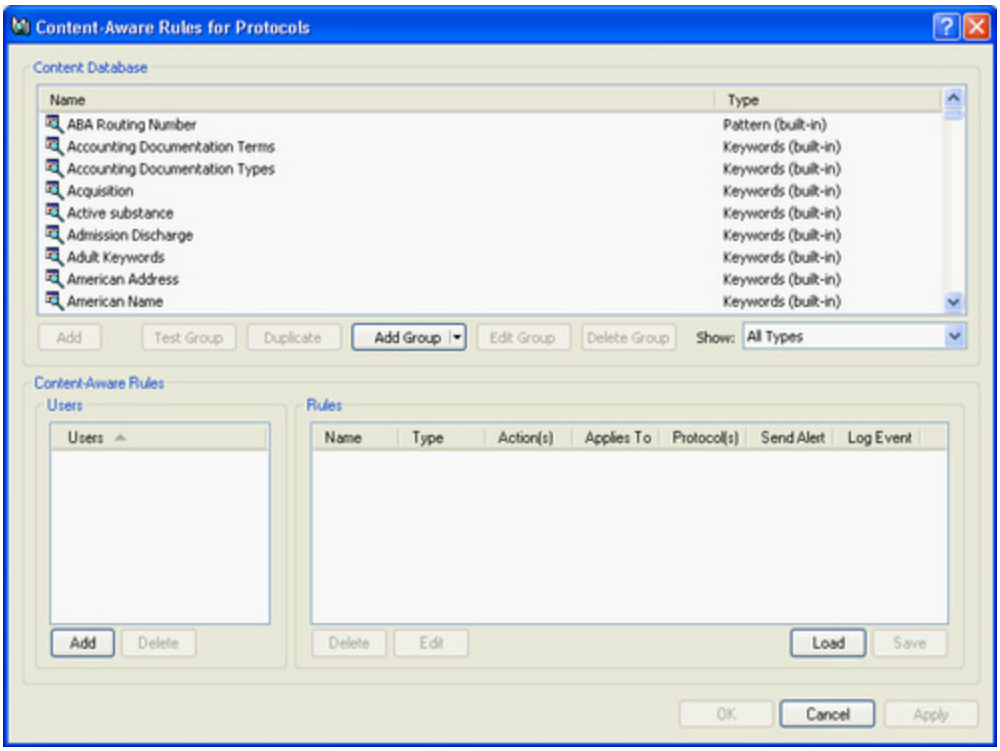
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

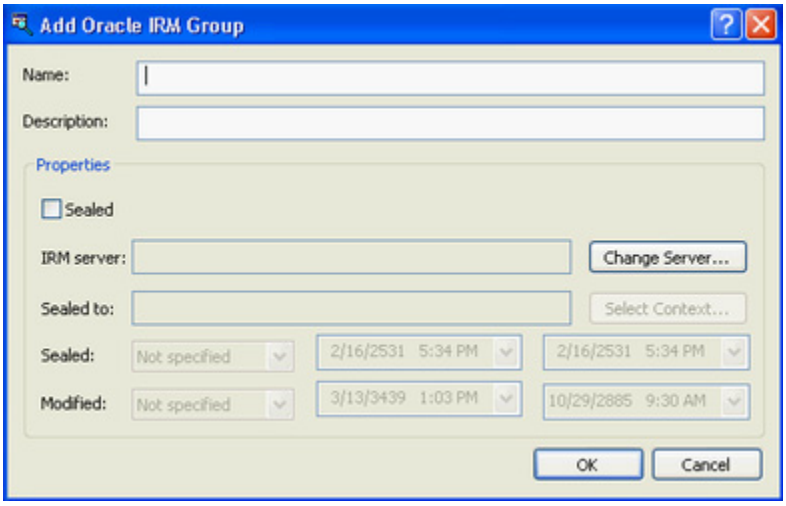
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

The Content-Aware Rules for Protocols dialog box appears.



4. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Oracle IRM**.

   The Add Oracle IRM Group dialog box appears.



5. In the **Add Oracle IRM Group** dialog box, do the following:

USE THIS	TO DO THIS
Name	Specify the name of the group.
Description:	Specify a description for the group.
Sealed	Detect and control access to documents that have been sealed using IRM. If you select the **Sealed** check box for an Oracle IRM group and then create a Content-Aware Rule based on this content group, this rule will control access to sealed documents.
IRM Server: Change Server	Specify or change the Oracle IRM server settings supported by DeviceLock Service. To do so, click **Change Server** to open the **Oracle IRM Server Settings** dialog box. In the **Oracle IRM Server Settings** dialog box, do the following: 1. In the **Server URL** box, specify the URL of the IRM server used to seal documents for which you want to control access. To remove the specified IRM server, click **Remove**. 2. In the **User name** box, specify the user account to use for authentication with the IRM server. 3. In the **Password** box, specify the password corresponding to the user account to use for authentication with the IRM server. 4. Click **Validate** to contact the specified IRM server and validate the URL against the one configured on the IRM Server. 5. Click **OK**.
Sealed to	Select the context(s) for which you want to control access. To do so, click **Select Context** to open the **Available contexts** dialog box. In the **Available contexts** dialog box, select the desired context, and then click **OK**. *To update the list of contexts, click Refresh*. *You can select multiple contexts by holding down the SHIFT key or the CTRL key while clicking them. The OR logic is applied to multiple*

USE THIS	TO DO THIS
	contexts specified within an Oracle IRM group. *You can also type multiple contexts separated by a semicolon (;) directly in the Sealed to box*.
Sealed	Specify the classification date/time of the sealed document. To do so, in the **Sealed** list, click any of the following options: • **Not specified** (this option is selected by default) • **Before than** Indicates that the document's classification date/time must be earlier than the specified date/time. • **After than** Indicates that the document's classification date/time must be later than the specified date/time. • **Between** Indicates that the document's classification date/time must fall within the specified date/time range. • **Not older than** Indicates that the document's classification date/time must not be older than the specified number of seconds, minutes, days, weeks, months, and years. • **Older than** Indicates that the document's classification date/time must be older than the specified number of seconds, minutes, days, weeks, months, and years.
Modified	Specify the last modification date/time of the sealed document. To do so, in the **Modified** list, click any of the following options: • **Not specified** (this option is selected by default) • **Before than** Indicates that the document's modified date/time must be earlier than the specified date/time. • **After than** Indicates that the document's modified date/time must be later than the specified date/time. • **Between** Indicates that the document's modified date/time must fall within the specified date/time range. • **Not older than** Indicates that the document's modified date/time must not be older than the specified number of seconds, minutes, days, weeks, months, and years. • **Older than** Indicates that the document's modified date/time must be older than the specified number of seconds, minutes, days, weeks, months, and years.

6. Click **OK** to close the **Add Oracle IRM Group** dialog box.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Protocols dialog box.

Viewing Built-in Content groups

You can view any built-in content groups but you cannot edit or delete them.

To view a built-in content group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Protocols dialog box appears.
4. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, select any built-in group you want to view, and then click **View Group**.

Duplicating Built-in Content groups

You cannot edit the built-in content groups but you can create and use their editable copies (duplicates) to suit your particular organization's needs.

To duplicate a built-in content group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.

- OR -

- Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

The Content-Aware Rules for Protocols dialog box appears.

4. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, select any built-in group you want to duplicate, and then click **Duplicate**.
5. In the dialog box that opens, edit the content group as required, and then click **OK**.

   The new content group you created is added to the existing list of content groups under Content Database in the upper pane of the Content-Aware Rules for Protocols dialog box.

Editing and Deleting Custom Content Groups

You can modify or delete custom content groups at any time.

To edit or delete a custom content group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.

     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Protocols dialog box appears.
4. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, select any custom group you want to edit or delete.
5. Click **Edit Group** to modify the selected content group. In the dialog box that opens, make the required changes, and then click **OK**.

   - OR -

   Click **Delete Group** or press the DELETE key to delete the selected content group.
6. In the **Content-Aware Rules for Protocols** dialog box, click **OK** or **Apply** to apply the changes.

Testing Content Groups

You can test any built-in or custom content group to see whether specified files match with it. By using these tests, you can verify that the rules that are created based on the content groups meet your specific business requirements.

To test a content group

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Protocols dialog box appears.
4. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, select any content group you want to test, and then click **Test Group**.

   You can test only one group at a time.

   The Open dialog box appears.
5. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to use for testing the specified content group.
6. In the folder list, locate and open the folder that contains the file.
7. Click the file, and then click **Open**.

   The Result message box is displayed. If the file matches with the specified content group, the Result message box contains the following text: "Selected file matches with the group." If the file does not match with the specified content group, the Result message box contains the following text: "Selected file does not match with the group."

   The maximum allowable file size is 5 MB. If your file exceeds 5 MB, you may receive the following error message: "File too large." This restriction applies only to DeviceLock WebConsole.

   When testing is in progress, the console stops responding (hangs)

Managing Content-Aware Rules

Managing Content-Aware Rules involves the following tasks:

- Defining Content-Aware Rules
- Editing Content-Aware Rules
- Copying Content-Aware Rules
- Exporting and importing Content-Aware Rules
- Undefining Content-Aware Rules
- Deleting Content-Aware Rules

You can manage Content-Aware Rules using DeviceLock Management Console, DeviceLock Group Policy Manager, or DeviceLock Service Settings Editor.

Defining Content-Aware Rules

Content-Aware Rules are created based on either the built-in or custom content groups. For detailed information on these groups, see "Configuring Content Detection Settings."

You can enable alerts that are sent when a specific Content-Aware Rule fires. Such alerts are enabled at the time you define a Content-Aware Rule.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific Content-Aware Rule, you must configure alert settings in **Service Options**.

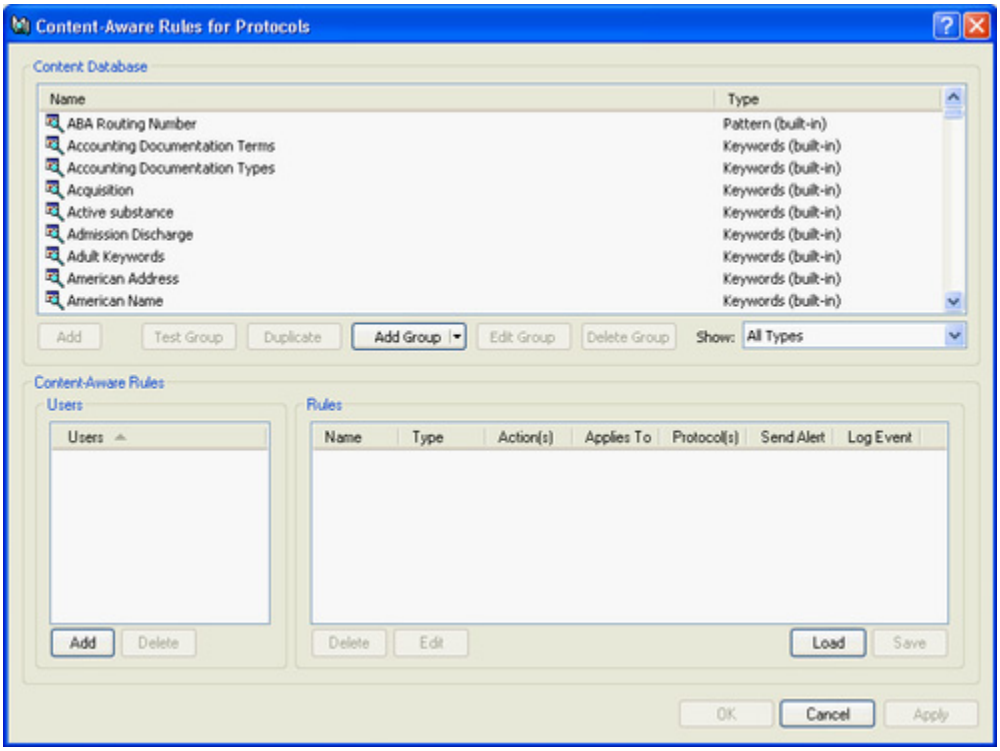
To define a Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

   The Content-Aware Rules for Protocols dialog box appears.



4. In the lower-left pane of the **Content-Aware Rules for Protocols** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Protocols dialog box.

   To delete a user or group, in the lower-left pane of the **Content-Aware Rules for Protocols** dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

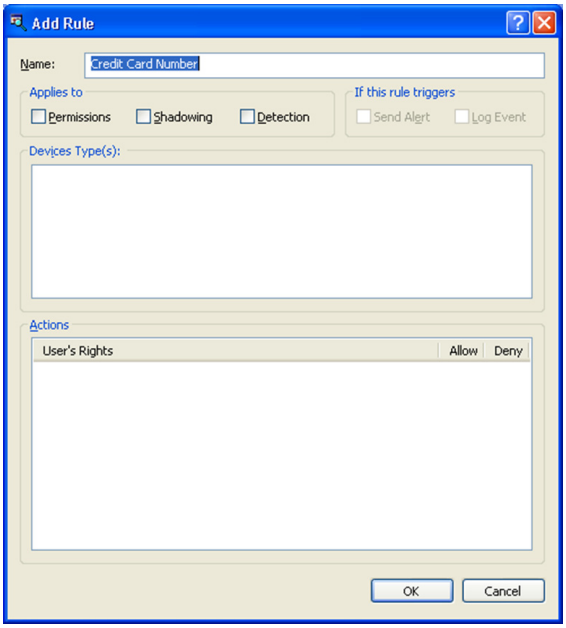
6. In the lower-left pane of the **Content-Aware Rules for Protocols** dialog box, under **Users**, select the users or groups for which you want to define the rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

7. In the upper pane of the **Content-Aware Rules for Protocols** dialog box, under **Content Database**, select the desired content group, and then click **Add**.

   Note: You can specify only one content group for a Content-Aware Rule.

   The Add Rule dialog box appears.



8. In the **Add Rule** dialog box, in the **Name** box, type the name of the Content-Aware Rule.

   By default, the Content-Aware Rule has the same name as the specified content group but you can enter a different name.

9. Under **Applies to**, specify the type of operation associated with the rule. The available options are:

   - **Permissions**: Specifies that the rule will apply to access control operations.
   - **Shadowing**: Specifies that the rule will apply to shadow copy operations.
   - **Detection**: Specifies that the rule will detect specified content in transferred data, log detection events, and send alerts to the administrator if the appropriate flags have been set.
   - **Permissions**, **Shadowing**: Specifies that the rule will apply to both access control and shadow copy operations.
   - **Permissions, Detection**: Specifies that the rule will apply to both access control and detection operations.
   - **Shadowing, Detection**: Specifies that the rule will apply to both shadow copy and detection operations.
   - **Permissions, Shadowing, Detection**: Specifies that the rule will apply to both access control and shadow copy operations, as well as to detection operations.

10. Under **If this rule triggers**, specify the following additional actions to be performed when the rule triggers:

    - **Send Alert**: Specifies that an alert is sent whenever the rule triggers.
    - **Log Event**: Specifies that an event is logged in the Audit Log whenever the rule triggers.

Note: Alerts and audit enabled for Content-Aware Rules have a priority over protocol-specific alerts and audit. For example, if you enable alerts and audit for a specific protocol and do not enable alerts and audit for a Content-Aware Rule associated with the same protocol, DeviceLock will not send an alert and will not log an event when the rule fires. For another example, if you enable alerts and audit for a Content-Aware Rule associated with a specific

protocol and do not enable alerts and audit for the same protocol, DeviceLock will send an alert and log an event when the rule fires.

11. Under **Protocol(s)**, select the appropriate protocol(s) you would like this rule to be applied to.

    Content-Aware Rules can be applied to the following protocols: File Sharing, FTP, HTTP, IBM Notes, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, MAPI, SMB, SMTP, Skype, Social Networks, Web Mail, Windows Messenger, and Yahoo Messenger.

    Under Action(s), if you multi-select protocols that have different combinations of configurable access rights, the dialog box will display the superset of access rights for the selection list: those that are common to all selected protocols, and those that do not necessarily apply to all protocols. As would be expected, if a particular access right that is displayed is not common to one or more particular selected protocols, it's setting will not/cannot be applied to those protocols and will only apply to protocols where the setting is supported.

12. Under **Action(s)**, specify which user actions are allowed or disallowed on protocols, which user actions are logged to the Shadow Log, and which user actions are detected.

    If the rule applies to shadow copy operations combined with other operations, the Read user right becomes unavailable. If the rule applies to detection operations combined with other operations, only Allow action becomes available. For detailed information on user rights and actions that can be specified in Content-Aware Rules, see "Content-Aware Rules for Access Control Operations", "Content-Aware Rules for Shadow Copy Operations" and "Content-Aware Rules for Detection Operations".

13. Click **OK**.

    The rule you created is displayed under Rules in the lower-right pane of the Content-Aware Rules for Protocols dialog box.

14. Click **OK** or **Apply** to apply the rule.

    The users or groups to which the Content-Aware Rule applies are displayed under Content-Aware Rules in the console tree. When you select a user or group to which a Content-Aware Rule applies in the console tree, in the details pane you can view detailed information regarding this rule. This information includes the following:

    - **Name** The name of the rule. By default, the rule has the same name as the specified content group.
    - **Type** The type of the content analysis. Possible values: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties, Complex** and **Oracle IRM**. **File Type Detection** indicates that recognition and identification of files is based on their characteristic signatures. **Keywords** indicates that recognition and identification of data/files is based on the specified keywords or phrases. **Pattern** indicates that recognition and identification of data/files is based on the specified patterns of text described by Perl regular expressions. **Document Properties** indicates that recognition and identification of files is based on their properties. **Complex** indicates that recognition and identification of data/files is based on the specified content described by a Boolean expression. **Oracle IRM** indicates that recognition and identification of files is based on their IRM contexts.

- **Action(s)** Shows which user actions are allowed or disallowed on protocols and which user actions are logged to the Shadow Log.
- **Applies To** Possible values: **Permissions**, **Shadowing**, **Detection**, **Permissions+Shadowing**, **Permissions+Detection**, **Shadowing+Detection**, **Permissions+Shadowing+Detection**. **Permissions** indicates that the rule applies to access control operations. **Shadowing** indicates that the rule applies to shadow copy operations. **Detection** indicates that the rule applies to detection operations. **Permissions+Shadowing** indicates that the rule applies to both access control and shadow copy operations. **Permissions+Detection** indicates that the rule applies to both access control and detection operations. **Shadowing+Detection** indicates that the rule applies to both shadow copy and detection operations. **Permissions+Shadowing+Detection** indicates that the rule applies to all available operations: access control, shadow copy, and detection.
- **Protocol(s)** The protocol(s) to which the rule applies.
- **Send Alert** Shows whether alerts are enabled or disabled for this rule.
- **Log Event** Shows whether audit logging of events associated with this rule is enabled or disabled.
- **Profile** Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to computers that are working offline.

  You can define different online vs. offline Content-Aware Rules for the same user or sets of users.

  For information about how to define offline Content-Aware Rules for protocols, see "Managing Offline Content-Aware Rules for Protocols."

Editing Content-Aware Rules

You can modify the Content-Aware Rule properties such as **Name**, **Applies To**, **If this rule triggers**, **Protocol(s)**, **Actions**.

To edit a Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Content-Aware Rules**, click **Manage**, and then do the following:

a) In the lower-left pane of the **Content-Aware Rules for Protocols** dialog box, under **Users**, select the user or group for which you want to edit the rule.

By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.

b) In the lower-right pane of the **Content-Aware Rules for Protocols** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.

- OR –

Right-click the rule, and then click **Edit**.

- OR -

Under **Protocols**, expand **Content-Aware Rules**, and then do the following:

a) Under **Content-Aware Rules**, select the user or group for which you want to edit the rule.

By selecting users or groups, you can view the Content-Aware Rules applied to them in the details pane.

b) In the details pane, right-click the rule you want to edit, and then click **Edit**.

- OR -

In the details pane, double-click the rule you want to edit.

The Edit Rule dialog box appears.

4. In the **Edit Rule** dialog box, modify the rule properties as required to meet your needs.
5. Click **OK** to apply the changes.

Copying Content-Aware Rules

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing Content-Aware Rules.

To copy a Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

- Right-click **Content-Aware Rules**, and then click **Manage**.
  - OR -
- Select **Content-Aware Rules**, and then click **Manage** on the toolbar.

The Content-Aware Rules for Protocols dialog box appears.

4. In the lower-left pane of the **Content-Aware Rules for Protocols** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.

   By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.

5. In the lower-right pane of the **Content-Aware Rules for Protocols** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

   The rule you cut or copy is automatically copied to the Clipboard.

   You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.

   To perform a drag-and-drop operation, select the rule and move it to the user or group to which you want to apply the copied rule.

6. In the lower-left pane of the **Content-Aware Rules for Protocols** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Protocols dialog box.

8. In the lower-left pane of the **Content-Aware Rules for Protocols** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

9. In the lower-right pane of the **Content-Aware Rules for Protocols** dialog box, right-click in the **Rules** pane and then click **Paste**.

   The copied rule is displayed under Rules in the lower-right pane of the Content-Aware Rules for Protocols dialog box.

10. Click **OK** or **Apply** to apply the copied rule.

Exporting and Importing Content-Aware Rules

You can export all your current Content-Aware Rules to a .cwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

To export Content-Aware Rules

1. If you use DeviceLock Management Console, do the following:

a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Save**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Save** on the toolbar.
     - OR -
   - Expand **Content-Aware Rules**, right-click any user or group to which the rule is applied, and then click **Save**.
     - OR -
   - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Save**.
     - OR -
   - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Save** on the toolbar.
     - OR -
   - Right-click **Content-Aware Rule**s, and then click **Manage**. In the lower-right pane of the **Content-Aware Rules for Protocols** dialog box, under **Rules**, click **Save**.

   The Save As dialog box appears.
4. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the .cwl file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.

   When you export rules, they are saved in a file with a .cwl extension.

To import Content-Aware Rules

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Load**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Load** on the toolbar.
     - OR -
   - Expand **Content-Aware Rules**, right-click any user or group to which the rule is applied, and then click **Load**.
     - OR -
   - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Load**.
     - OR -
   - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Load** on the toolbar.
     - OR -
   - Right-click **Content-Aware Rules**, and then click **Manage**. In the lower-right pane of the **Content-Aware Rules for Protocols** dialog box, under **Rules**, click **Load**.

   The Open dialog box appears.
4. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
5. In the folder list, locate and open the folder that contains the file.
6. Click the file, and then click **Open**.

   You can import only one .cwl file at a time.

Undefining Content-Aware Rules

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent Content-Aware Rules from being applied to a specific group of client computers. To do so, you need to return the previously defined Content-Aware Rules to the unconfigured state. All undefined DeviceLock settings are ignored by client computers.

To undefine Content-Aware Rules

1. If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.

b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined DeviceLock policies.
c) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, right-click **Content-Aware Rules**, and then click **Undefine**.

Deleting Content-Aware Rules

You can delete individual Content-Aware Rules when they are no longer required.

To delete a Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Expand **Content-Aware Rules**, right-click the user or group to which the rule is applied, and then click **Delete user**.
     When you delete a user or group, the rule associated with this user or group is automatically deleted.

     - OR -
   - Expand **Content-Aware Rules**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.
     - OR -

- Right-click **Content-Aware Rules**, and then click **Manage**. In the lower-left pane of the **Content-Aware Rules for Protocols** dialog box, under **Users**, select the user or group to which the rule is applied. In the lower-right pane of the **Content-Aware Rules for Protocols** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.
  You can select multiple rules that you want to delete by holding down the SHIFT key or the CTRL key while clicking them.

Protocols (Regular Profile)

DeviceLock allows you to control data that is transferred over different network protocols, thus enhancing protection against unwanted information disclosure and offering additional transport-level security. With the Protocols feature, you can define policies to selectively allow or block data/file transmission via specific protocols as well as shadow copy the transferred data. For flexibility, policies can be defined on a per-user or per-group basis.

DeviceLock provides control over the following protocols and Web applications:

- **File Sharing** – controls the exchange of information via Web-based file storage, sharing and synchronization services such as Amazon Simple Storage Service (Amazon S3), Dropbox, Box, Google Docs/Google Drive, Rusfolder (Rusfolder.com, former iFolder.ru), OneDrive, Yandex.Disk, iCloud and Cloud Mail.ru.
  Both non-SSL and SSL connections are supported.
- **FTP** (File Transfer Protocol) – the Internet standard protocol for transferring files between computers.
  Both active-mode and passive-mode FTP connections are supported. FTPS (FTP over SSL) is also supported. Both implicit and explicit FTPS connections are supported.
- **HTTP** (Hypertext Transfer Protocol) – an application-level client/server protocol used to transfer information over the World Wide Web.
  HTTPS (SSL over HTTP) is also supported.
- **IBM Notes** – a proprietary protocol that IBM Notes uses to communicate with IBM Domino server. DeviceLock supports version 8.5 (December 2008) and later versions (any client-server combinations that Domino / Notes support).
- **ICQ/ AOL Messenger** – AOL's Open System for Communication in Realtime (OSCAR) protocol used by ICQ and AOL Instant Messenger (AIM).
  Both non-SSL and SSL connections are supported.
- **IRC** (Internet Relay Chat) – an Internet standard protocol that supports interactive, real-time, text-based communications in established "chat rooms" on the Internet by means of IRC servers.
  Both non-SSL and SSL connections are supported.
- **Jabber** – an open, XML-based protocol for instant messaging. Jabber is also known as XMPP, the Extensible Messaging and Presence Protocol.
- **Mail.ru Agent** – an instant messaging program created by Mail.ru.

  Note: SSL connections between Jabber/Mail.ru Agent clients and the server are controlled as generic (non-SSL) connections.

- **MAPI** (Messaging Application Programming Interface) – MAPI/RPC (also known as Outlook - Exchange Transport Protocol) is the proprietary protocol that Microsoft Outlook uses to communicate with Microsoft Exchange Server. DeviceLock supports Outlook 2003, Outlook 2007, Outlook 2010, Outlook 2013 (both 64-bit and 32-bit versions) and all versions of Exchange Server.

- **Skype** – a proprietary voice-over-Internet Protocol service and software application. DeviceLock supports Skype version 4.x and later.
- **SMB** (Server Message Block) – a network file sharing protocol.
- **SMTP** (Simple Mail Transfer Protocol) – an Internet standard protocol used for exchanging e-mail messages between SMTP servers on the Internet.
  Extended SMTP (ESMTP) is also supported. Both non-SSL and SSL connections are supported.
- **Social Networks** – controls communication with social networking sites. The following social networking sites are supported: Facebook (+API), Twitter, Google+, LinkedIn, Tumblr, MySpace, Vkontakte (+API), XING.com, LiveJournal, MeinVZ.de, StudiVZ.de, Disqus, LiveInternet.ru, Odnoklassniki.ru.

  Note: SSL traffic on social networking sites is controlled as generic (non-SSL) traffic.
- **Telnet** – the Internet standard protocol for remote terminal connection service.
- **Torrent** – controls peer-to-peer (P2P) communications of torrent clients over TCP, UDP or HTTP protocols.
- **Web Mail** – controls Web-based mail communication. The following Web-based e-mail services are supported: Gmail, Yahoo! Mail, Hotmail (Outlook.com), AOL Mail, GMX.de, Web.de, Mail.ru, Outlook Web App (OWA), Rambler Mail, Yandex Mail.
  Both non-SSL and SSL connections are supported.
- **WhatsApp Web** – controls the web client of the WhatsApp instant messaging application.
- **Windows Messenger** – Microsoft Notification Protocol (MSNP), the underlying protocol used by Windows Live Messenger and Windows Messenger.
- **Yahoo Messenger** – the underlying network protocol used by the Yahoo! Messenger instant messaging client for Yahoo!

Note: The SSL protocol is used in the Protocols White List to allow applications with embedded SSL certificates to connect to their servers.

You can manage protocol security policies by using DeviceLock Management Console, Service Settings Editor, or DeviceLock Group Policy Manager. You can also use the Report Permissions/Auditing plug-in in DeviceLock Enterprise Server to view and change security policies defined for protocols. For more information, see "Report Permissions/Auditing."

Managing Permissions for Protocols

To govern the exchange of information at the transport level, configure access to communications protocols by setting appropriate permissions. These permissions specify who can gain access to which protocols and what level of access users have. Permissions can be set on a per-user or per-group basis.

The following table describes access rights available for permissions associated with protocols.

PROTOCOL	ACCESS RIGHTS
File Sharing	**Generic: Send/Receive Data** The right to access a file sharing site, to browse its contents and to download files. **Generic: POST Requests** The right to submit Web form data, such as user comments to specific files. This right does not control the login information entered into the username and password form. **Generic: Outgoing Files** The right to upload files to a file sharing site. **SSL: Send/Receive Data** The right to access a file sharing site, to browse its contents and to download files using SSL. **SSL: POST Requests** The right to submit Web form data, such as user comments to specific files using SSL. This right does not control the login information entered into the username and password form. **SSL: Outgoing Files** The right to upload files to a file sharing site using SSL.
FTP	**Generic: Send/Receive Data** The right to connect to an FTP server, send and receive protocol data, download files from an FTP server. **Generic: Outgoing Files** The right to upload files to an FTP server. **SSL: Send/Receive Data** The right to connect to an FTP server, send and receive protocol data, download files from an FTP server using FTPS. **SSL: Outgoing Files** The right to upload files to an FTP server using FTPS.
HTTP	**Generic: Send/Receive Data** The right to connect to a Web server, send and receive protocol data, web pages and objects on web pages (such as scripts, Flash files, JPEG, PNG, and GIF images, etc.), and download files. **Generic: POST Requests** The right to submit Web form data to a Web server using HTTP. **Generic: Outgoing Files** The right to upload files to a Web server using HTTP. **SSL: Send/Receive Data** The right to connect to a Web server, send and receive protocol data, web pages and objects on web pages (such as scripts, Flash files, JPEG, PNG, and GIF images, etc.), and download files using HTTPS. **SSL: POST Requests** The right to submit Web form data to a Web server using HTTPS. **SSL: Outgoing Files** The right to upload files to a Web server using HTTPS.
IBM Notes	**Generic: Send/Receive Data** The right to connect the IBM Notes client to IBM Domino server and read e-mail. **Generic: Outgoing Messages** The right to send e-mail messages without attachments from the IBM Notes client to IBM Domino server. **Generic: Outgoing Files** The right to send e-mail attachments from the IBM Notes client to IBM Domino server.
ICQ/AOL Messenger	**Generic: Send/Receive Data, Outgoing Messages** The right to connect to the ICQ and AOL Instant Messenger server and to send and receive instant messages and receive files.

PROTOCOL	ACCESS RIGHTS
	Generic: Outgoing Files The right to send files. **SSL: Send/Receive Data, Outgoing Messages** The right to connect to the ICQ and AOL Instant Messenger server and to send and receive instant messages and receive files using SSL. **SSL: Outgoing Files** The right to send files using SSL.
IRC	**Generic: Send/Receive Data, Outgoing Messages** The right to connect to an IRC server and to send and receive instant messages and receive files. **Generic: Outgoing Files** The right to send files. **SSL: Send/Receive Data, Outgoing Messages** The right to connect to an IRC server and to send and receive instant messages and receive files using SSL. **SSL: Outgoing Files** The right to send files using SSL.
Jabber	**Generic: Send/Receive Data**, **Outgoing Messages** The right to connect to a Jabber server and to send and receive instant messages and receive files. **Generic: Outgoing Files** The right to send files.
Mail.ru Agent	**Generic: Send/Receive Data, Outgoing Messages** The right to connect Mail.ru Agent to the Mail.ru server and to send and receive instant messages and receive files. **Generic: Outgoing Files** The right to send files.
MAPI	**Generic: Send/Receive Data** The right to connect the Outlook client to Microsoft Exchange Server and read e-mail. **Generic: Outgoing Messages** The right to send e-mail messages without attachments from the Outlook client to Microsoft Exchange Server. **Generic: Outgoing Files** The right to send e-mail attachments from the Outlook client to Microsoft Exchange Server.
Skype	**Generic: Send/Receive Data** The right to connect to the Skype server and receive instant messages and files. **Generic: Incoming Calls** The right to receive calls. **Generic: Outgoing Calls** The right to make calls. **Generic: Outgoing Messages** The right to send instant messages. **Generic: Outgoing Files** The right to send files.
SMB	**Generic: Send/Receive Data** The right to access shared resources on an SMB server and to download files/folders. Also, this right allows users of external computers to connect to, browse the content of and transfer data to locally shared resources on the computer where DeviceLock Service runs. **Generic: Outgoing Files** The right to upload files to an SMB server. Also, this right allows users of external computers to read local files/folders shared on the computer where DeviceLock Service runs.
SMTP	**Generic: Send/Receive Data** The right to connect to an SMTP server and to send and receive protocol data. **Generic: Outgoing Messages** The right to send e-mail messages without attachments.

PROTOCOL	ACCESS RIGHTS
	Generic: Outgoing Files The right to send e-mail attachments. **SSL: Send/Receive Data** The right to connect to an SMTP server and to send and receive protocol data using SSL. **SSL: Outgoing Messages** The right to send e-mail messages without attachments using SSL. **SSL: Outgoing Files** The right to send e-mail attachments using SSL.
Social Networks	**Generic: Send/Receive Data** The right to have view access to a social networking site. **Generic: Outgoing Messages** The right to send messages, comments, posts, etc. **Generic: Outgoing Files** The right to upload media and file content to a social networking site.
Telnet	**Generic: Send/Receive Data** The right to connect to a Telnet server and to send and receive protocol data.
Torrent	**Generic: Send/Receive Data** The right to connect to remote hosts.
Web Mail	**Generic: Send/Receive Data** The right to access Webmail and read e-mail. **Generic: Outgoing Messages** The right to send e-mail messages without attachments. **Generic: Outgoing Files** The right to send e-mail attachments. **SSL: Send/Receive Data** The right to access Webmail and read e-mail using SSL. **SSL: Outgoing Messages** The right to send e-mail messages without attachments using SSL. **SSL: Outgoing Files** The right to send e-mail attachments using SSL.
WhatsApp Web	**Generic: Send/Receive Data** The right to access WhatsApp Web host (web.whatsapp.com).
Windows Messenger	**Generic: Send/Receive Data, Outgoing Messages** The right to connect to the Windows Messenger server and to send and receive instant messages and receive files. **Generic: Outgoing Files** The right to send files.
Yahoo Messenger	**Generic: Send/Receive Data, Outgoing Messages** The right to connect to the Yahoo Messenger server and to send and receive instant messages and receive files. **Generic: Outgoing Files** The right to send files.

Note: You can define different online vs. offline permissions on protocols for the same user or sets of users. Online permissions (Regular Profile) apply to client computers that are working online. Offline permissions (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define offline permissions for protocols, see "Managing Offline Permissions for Protocols."

The **POST Requests** access right for the **File sharing** protocol, when applied to the iCloud service, controls whether a user can upload non-file data (Mail, Notes, Calendar, Contacts, Reminders) to iCloud. The same access right enables audit logging and shadow copying of the non-file data uploaded to iCloud. Audit records of upload attempts and shadow copies of that data are stored as **Outgoing Messages.**

You can set the default permissions on protocols for both types of profiles (Regular Profile and Offline Profile). The default permissions are assigned to the Administrators and Everyone accounts. The following table lists access rights granted to these accounts by default.

ACCOUNT/ PROTOCOL	ADMINISTRATORS	EVERYONE
File Sharing	Generic: Send/Receive Data, POST Requests, Outgoing Files. SSL: Send/Receive Data, POST Requests, Outgoing Files	Generic: Send/Receive Data, POST Requests. SSL: Send/Receive Data, POST Requests
FTP	Generic: Send/Receive Data, Outgoing Files SSL: Send/Receive Data, Outgoing Files	Generic: Send/Receive Data SSL: Send/Receive Data
HTTP	Generic: Send/Receive Data, POST Requests, Outgoing Files SSL: Send/Receive Data, POST Requests, Outgoing Files	Generic: Send/Receive Data, POST Requests SSL: Send/Receive Data, POST Requests
IBM Notes	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
ICQ/AOL Messenger	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
IRC	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
Jabber	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
Mail.ru Agent	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
MAPI	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages

ACCOUNT/ PROTOCOL	ADMINISTRATORS	EVERYONE
Skype	Generic: Send/Receive Data, Incoming Calls, Outgoing Messages, Outgoing Files, Outgoing Calls	Generic: Send/Receive Data, Incoming Calls, Outgoing Messages, Outgoing Calls
SMB	Generic: Send/Receive Data, Outgoing Files	Generic: Send/Receive Data
SMTP	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
Social Networks	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
Telnet	Generic: Send/Receive Data	Generic: Send/Receive Data
Torrent	Generic: Send/Receive Data	Generic: Send/Receive Data
Web Mail	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
WhatsApp Web	Generic: Send/Receive Data	Generic: Send/Receive Data
Windows Messenger	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
Yahoo Messenger	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages

Managing online (regular) permissions for protocols involves the following tasks:

- Setting and editing permissions.
- Undefining permissions.

Online permissions for protocols can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that permissions on a protocol are not set.
Configured	Indicates that permissions on a protocol are set.
Full Access	Indicates that full access rights are granted to the Everyone account.
No Access	Indicates one of the following: • The Everyone account has No Access permissions and is the only account

STATE	DESCRIPTION
	assigned to a protocol. *No Access permissions assigned to the Everyone account take priority over permissions assigned to other accounts*. • All users and groups assigned to a protocol have No Access permissions. • All users and groups assigned to a protocol are removed.

Setting and Editing Permissions

To set and edit permissions

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Permissions**.

   When you select Permissions in the console tree, in the details pane you can view protocols for which you can set permissions. In the details pane, you can also view the current state of online (regular) permissions for each protocol in the Regular column.
4. In the details pane, do one of the following:
   - Right-click the protocol for which you want to set or edit permissions, and then click **Set Permissions**.
     - OR -
   - Select the protocol for which you want to set or edit permissions, and then click **Set Permissions** on the toolbar.

   You can select several protocols for which you want to set the same permissions by holding down the SHIFT key or the CTRL key while clicking them.

Note: When selecting several protocols that have different access rights, consider the following:

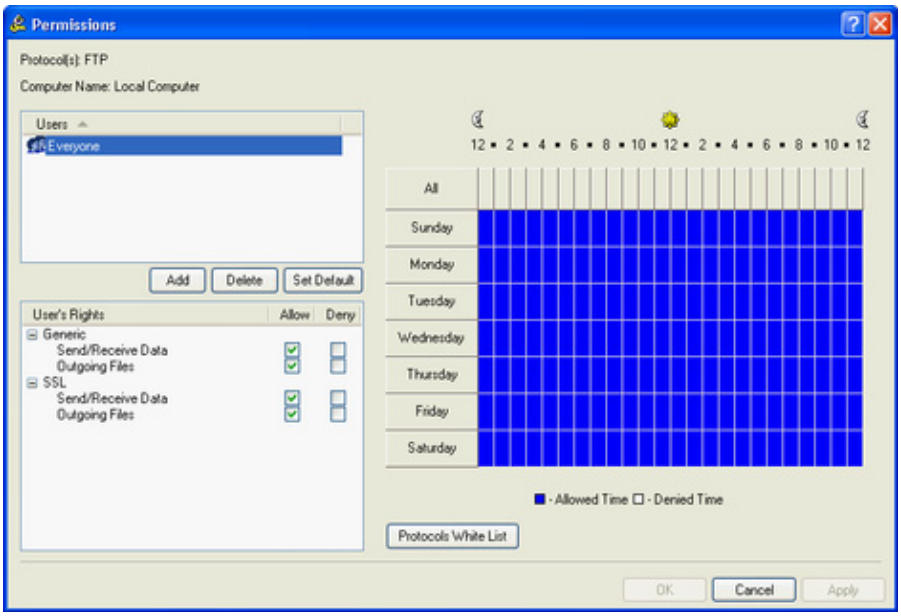
The **Permissions** dialog box displays only those access rights that are common to all selected protocols.

If all access rights displayed in the **Permissions** dialog box are allowed for the specified users, these users will have full access to the selected protocols.

If all access rights displayed in the **Permissions** dialog box are denied for the specified users, these users will have no access to the selected protocols.

Some access rights depend on other rights. If you grant a right that requires another right, the required right is granted automatically. For example, if you grant only the **Generic: Outgoing Files** right for the Social Networks and Web Mail protocols, the following rights are granted automatically: **Generic: Send/Receive Data**, **Generic: Outgoing Messages**, **Generic: Outgoing Files**.

The Permissions dialog box appears.



5. In the **Permissions** dialog box, do the following:

TO DO THIS	FOLLOW THESE STEPS
To set the default permissions	• In the upper-left pane of the dialog box, under **Users**, click **Set Default**. *The default permissions are assigned to the Administrators, and Everyone accounts. For information about which permissions are set for these accounts by default, see "Managing Permissions for Protocols."*
To set permissions for an additional user or group	1. In the upper-left pane of the dialog box, under **Users**, click **Add**. *The Select Users or Groups dialog box appears.* 2. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**. *The users and groups that you added are displayed under Users in the upper-left pane of the Permissions dialog box.* 3. In the upper-left pane of the **Permissions** dialog box, under **Users**, select the user or group. *You can select multiple users and/ or groups by holding down the SHIFT key or the CTRL key while clicking them.* 4. In the lower-left pane of the **Permissions** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or

TO DO THIS	FOLLOW THESE STEPS
	deny the appropriate access rights. *In the right pane of the Permissions dialog box, you can set day and time restrictions that narrow user access to the specified protocol(s). Use the left mouse button to select days and hours when the selected user or group will have access to the specified protocol(s). Use the right mouse button to mark days and hours when the selected user or group will not have access to the specified protocol(s).*
To change permissions for an existing user or group	1. In the upper-left pane of the dialog box, under **Users**, select the user or group. 2. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate access rights.
To remove an existing user or group and permissions	• In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

6. Click **OK** or **Apply**.

Undefining Permissions

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent some or all of the previously set permissions for protocols from being applied to a specific group of client computers. To do so, you need to return the previously set permissions to the unconfigured state. All undefined DeviceLock settings are ignored by client computers.

To undefine permissions

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock.**
2. Expand **Protocols**.
3. Under **Protocols**, select **Permissions**.

   When you select Permissions in the console tree, in the details pane you can view protocols for which you can set permissions.
4. In the details pane, right-click the protocol whose permissions you want to undefine, and then click **Undefine**.

You can undefine permissions for multiple protocols at the same time. To do this, do the following:

a) In the details pane, select multiple protocols by holding down the SHIFT key or the CTRL key while clicking them.
b) Right-click the selection, and then click **Undefine**.

Managing Audit, Shadowing and Alerts for Protocols

DeviceLock provides the capability to audit and shadow copy data/file transfers via different protocols. Auditing and shadow copying are used to monitor and record security-critical data transfer operations. Regular analysis of log data is an effective way to detect and trace misuse of sensitive information and data breach incidents caused by data loss or theft.

For auditing and shadow copying at the transport level, DeviceLock uses two types of logging: Audit Logs and Shadow Logs. The Audit Log is used to audit access to protocols and track what individual users do. Audit data can be written to the Windows Event Log, to the DeviceLock proprietary log, or both. To define what log should be used, set the Audit log type parameter in Service Options. To view audit log data, use either DeviceLock Service Audit Log Viewer or DeviceLock Enterprise Server Audit Log Viewer.

The Shadow Log is used to store a full copy of data/files transferred via specified protocols. To view shadow log data, use either DeviceLock Service Shadow Log Viewer or DeviceLock Enterprise Server Shadow Log Viewer.

Auditing and shadow copying of data transferred via specified protocols are enabled by defining audit and shadowing rules. Each rule associated with a protocol specifies users or groups the rule applies to and appropriate audit/shadowing rights which determine which user actions to audit/shadow copy.

Audit events logged include a variety of information such as the event type, the date and time of the event, the associated protocol, the user associated with this event, process information and event-specific information.

The following table provides summary information on audit and shadowing rights that can be specified in rules and describes event-specific information that is written to the log.

PROTOCOL	AUDIT/SHADOWING RIGHTS
File Sharing	**Audit: Connection** – Enables audit logging of user attempts to connect to a file sharing site. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log*. **Audit: Incoming Files** – Enables audit logging of user attempts to download a file from a file sharing site. *The Incoming File action, the download link, the IP address with the port number and the name of the host, the name of the protocol are written to the log*.

PROTOCOL	AUDIT/SHADOWING RIGHTS
	Audit: POST Requests – Enables audit logging of user attempts to submit Web form data, such as user comments to specific files. *The POST Request action, the name of the file storage, sharing and synchronization service, the IP address with the port number and the name of the host, the name of the protocol are written to the log*. **Audit: Outgoing Files** – Enables audit logging of user attempts to upload a file to a file sharing site. *The Outgoing File action, the name of the file, the IP address with the port number and the name of the host, the name of the protocol are written to the log*. **Shadowing: Incoming Files** – Enables shadow copying of files downloaded from a file sharing site. *Shadow copies of downloaded files are written to the log*. **Shadowing: POST Requests** – Enables shadow copying of data (user comments to specific files) entered into Web forms. *Shadow copies of data entered into Web forms are written to the log*. **Shadowing: Outgoing Files** – Enables shadow copying of files uploaded to a file sharing site. *Shadow copies of uploaded files are written to the log*. **Note:** The **POST Requests** access right for the **File Sharing** protocol, when applied to the iCloud service, enables audit logging and shadow copying of non-file data (Mail, Notes, Calendar, Contacts, Reminders).
FTP	**Audit: Connection** – Enables audit logging of user attempts to connect to an FTP site. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log*. **Audit: Incoming Files –** Enables audit logging of user attempts to download a file from an FTP site. *The Incoming File action, the absolute path and complete name of the file (for example, ftp://myftp/myfile.doc), the IP address with the port number and the name of the host are written to the log*. **Audit: Outgoing Files –** Enables audit logging of user attempts to upload a file to an FTP site. *The Outgoing File action, the absolute path and complete name of the file (for example, ftp://myftp/myfile.doc), the IP address with the port number and the name of the host are written to the log*. **Shadowing: Incoming Files –** Enables shadow copying of files downloaded from an FTP site. *Shadow copies of downloaded files are written to the log*. **Shadowing: Outgoing Files –** Enables shadow copying of files uploaded to an FTP site.

PROTOCOL	AUDIT/SHADOWING RIGHTS
	Shadow copies of uploaded files are written to the log.
HTTP	**Audit: Connection** – Enables audit logging of user attempts to open a web page. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log*. **Note:** When this right is enabled, numerous Connection events are recorded in the Audit Log each time a user attempts to open a web page. This happens because a web page often requests resources (such as images, scripts, etc.) from other hosts. **Audit: Incoming Data** – Enables audit logging of web pages and objects on web pages: scripts, Flash files (up to 1.5 MB in size), images (up to 512 KB in size), text (up to 200 KB in size), etc. *The Incoming Data action, the URL of the web page and objects on the web page, the IP address with the port number and the name of the host are written to the log*. **Audit: Incoming Files** – Enables audit logging of user attempts to download a file from a Web site. *The Incoming File action, the absolute path and complete name of the file (for example, http://domain/path/myfile.doc), the IP address with the port number and the name of the host are written to the log*. **Audit: Outgoing Data** – The Outgoing Data content type contains no data. This right enables audit logging of blocked user attempts to open a web page, if the **Audit Denied** option is set for the protocol. *The Outgoing Data action, the URL of the web page and objects on the web page, the IP address with the port number and the name of the host are written to the log*. **Audit: POST Requests –** Enables audit logging of user attempts to submit Web form data to a Web site. *The POST Request action and the URL of the script that sent the POST request are written to the log*. **Audit: Outgoing Files** – Enables audit logging of user attempts to upload a file to a Web site. *The Outgoing File action, the absolute path and complete name of the file (for example, http://domain/path/myfile.doc), the IP address with the port number and the name of the host are written to the log*. **Shadowing: Incoming Data** – Enables shadow copying of web pages and objects on web pages: scripts, Flash files (up to 1.5 MB in size), images (up to 512 KB in size), text (up to 200 KB in size), etc. *Shadow copies of web pages and their constituent components are written to the log*. **Shadowing: Incoming Files** – Enables shadow copying of files downloaded from a Web site. *Shadow copies of downloaded files are written to the log*. **Shadowing: Outgoing Data** – This right has no impact on shadow copying.

PROTOCOL	AUDIT/SHADOWING RIGHTS
	Shadowing: POST Requests – Enables shadow copying of data entered into Web forms. *Shadow copies of data entered into Web forms are written to the log*. **Shadowing: Outgoing Files** – Enables shadow copying of files uploaded to a Web site. *Shadow copies of uploaded files are written to the log*.
IBM Notes	**Audit: Connection** – Enables audit logging of user attempts to connect the IBM Notes client to IBM Domino server. *The Connection action and the IP address or the name of the host are written to the log. A successful connection to the IBM Domino Server can generate several Connection events*. **Audit: Incoming Messages, Incoming Files** - Enables audit logging of user attempts to receive an e-mail message with or without attachments from IBM Domino server to the IBM Notes client. *The Incoming Message action, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender=>recipient1, recipient2)*. **Audit: Outgoing Messages, Outgoing Files** – Enables audit logging of user attempts to send an e-mail message with or without attachments from the IBM Notes client to IBM Domino server. *The Outgoing Message action, the number of attachments, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender=>recipient1, recipient2)*. *The number of attachments is written to the Audit Log only when a Content-Aware Rule for the protocol was used to inspect the e-mail message.* **Shadowing: Incoming Messages, Incoming Files** – Enables shadow copying of received e-mail messages with or without attachments. *Shadow copies of received e-mail messages with or without attachments are written to the log as .eml files. You can, for example, open .eml files in Microsoft Outlook Express, in Windows Mail, and in Mozilla Thunderbird*. **Shadowing: Outgoing Messages, Outgoing Files** – Enables shadow copying of sent e-mail messages with or without attachments. *Shadow copies of sent e-mail messages with or without attachments are written to the log as .eml files. You can, for example, open .eml files in Microsoft Outlook Express, in Windows Mail, and in Mozilla Thunderbird*. *The number of attachments is always written to the Shadow Log*.
ICQ/AOL Messenger	**Audit: Connection** – Enables audit logging of user attempts to connect to the ICQ and AOL Instant Messenger server. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log*. **Audit: Incoming Messages**, **Outgoing Messages** – Enables audit logging of user attempts to send and receive instant messages. *The Chat action, IDs of all IM participants, the IP address with the port number and the name of the host are written to the log. The ID of the local participant*

PROTOCOL	AUDIT/SHADOWING RIGHTS
	precedes the ID of a remote participant. **Audit: Incoming Files** - Enables audit logging of user attempts to receive a file. *The Incoming File action and the name of the file are written to the log*. **Audit: Outgoing Files** - Enables audit logging of user attempts to send a file. *The Outgoing File action and the name of the file are written to the log*. **Shadowing: Incoming Messages** – Enables shadow copying of received instant messages. *Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all received messages.* **Shadowing: Incoming Files** – Enables shadow copying of received files. *Shadow copies of received files are written to the log*. **Shadowing: Outgoing Messages** – Enables shadow copying of sent instant messages. *Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all sent messages*. **Shadowing: Outgoing Files** – Enables shadow copying of sent files. *Shadow copies of sent files are written to the log*.
IRC	**Audit: Connection** – Enables audit logging of user attempts to connect to an IRC server. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log*. **Audit: Incoming Messages**, **Outgoing Messages** – Enables audit logging of user attempts to send and receive instant messages. *The Chat action, IDs of all IM participants, the IP address with the port number and the name of the host are written to the log. The ID of the local participant precedes the ID of a remote participant*. **Audit: Incoming Files** - Enables audit logging of user attempts to receive a file. *The Incoming File action and the name of the file are written to the log*. **Audit: Outgoing Files** - Enables audit logging of user attempts to send a file. *The Outgoing File action and the name of the file are written to the log*. **Shadowing: Incoming Messages** – Enables shadow copying of received instant messages. *Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all received messages.* **Shadowing: Incoming Files** – Enables shadow copying of received files.

PROTOCOL	AUDIT/SHADOWING RIGHTS
	Shadow copies of received files are written to the log. **Shadowing: Outgoing Messages** – Enables shadow copying of sent instant messages. *Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all sent messages*. **Shadowing: Outgoing Files** – Enables shadow copying of sent files. *Shadow copies of sent files are written to the log*.
Jabber	**Audit: Connection** – Enables audit logging of user attempts to connect to a Jabber server. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log*. **Audit: Incoming Messages**, **Outgoing Messages** – Enables audit logging of user attempts to send and receive instant messages. *The Chat action, IDs of all IM participants, the IP address with the port number and the name of the host are written to the log. The ID of the local participant precedes the ID of a remote participant*. **Audit: Incoming Files** - Enables audit logging of user attempts to receive a file. *The Incoming File action and the name of the file are written to the log*. **Audit: Outgoing Files** - Enables audit logging of user attempts to send a file. *The Outgoing File action and the name of the file are written to the log*. **Shadowing: Incoming Messages** – Enables shadow copying of received instant messages. *Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all received messages.* **Shadowing: Incoming Files** – Enables shadow copying of received files. *Shadow copies of received files are written to the log*. **Shadowing: Outgoing Messages** – Enables shadow copying of sent instant messages. *Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all sent messages*. **Shadowing: Outgoing Files** – Enables shadow copying of sent files. *Shadow copies of sent files are written to the log*.
Mail.ru Agent	**Audit: Connection –** Enables audit logging of user attempts to connect Mail.ru Agent to the Mail.ru server. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name*

PROTOCOL	AUDIT/SHADOWING RIGHTS
	resolution fails, the host name is not written to the log. **Audit: Incoming Messages**, **Outgoing Messages** – Enables audit logging of user attempts to send and receive instant messages. *The Chat action, IDs of all IM participants, the IP address with the port number and the name of the host are written to the log. The ID of the local participant precedes the ID of a remote participant*. **Audit: Incoming Files** - Enables audit logging of user attempts to receive a file. *The Incoming File action and the name of the file are written to the log*. **Audit: Outgoing Files** - Enables audit logging of user attempts to send a file. *The Outgoing File action and the name of the file are written to the log*. **Shadowing: Incoming Messages** – Enables shadow copying of received instant messages. *Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all received messages.* **Shadowing: Incoming Files** – Enables shadow copying of received files. *Shadow copies of received files are written to the log*. **Shadowing: Outgoing Messages** – Enables shadow copying of sent instant messages. *Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all sent messages*. **Shadowing: Outgoing Files** – Enables shadow copying of sent files. *Shadow copies of sent files are written to the log*.
MAPI	**Audit: Connection** – Enables audit logging of user attempts to connect the Outlook client to Microsoft Exchange Server. *The Connection action and the IP address or the name of the host are written to the log. A successful connection to the Microsoft Exchange Server can generate several Connection events*. **Audit: Incoming Messages, Incoming Files** - Enables audit logging of user attempts to receive an e-mail message with or without attachments from Microsoft Exchange Server to the Outlook client. *The Incoming Message action, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender=>recipient1, recipient2)*. **Audit: Outgoing Messages, Outgoing Files** – Enables audit logging of user attempts to send an e-mail message with or without attachments from the Outlook client to Microsoft Exchange Server. *The Outgoing Message action, the number of attachments, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender=>recipient1, recipient2)*. *The number of attachments is written to the Audit Log only when a Content-*

PROTOCOL	AUDIT/SHADOWING RIGHTS
	Aware Rule for the protocol was used to inspect the e-mail message. **Shadowing: Incoming Messages, Incoming Files** – Enables shadow copying of received e-mail messages with or without attachments. *Shadow copies of received e-mail messages with or without attachments are written to the log as .eml files. You can, for example, open .eml files in Microsoft Outlook Express, in Windows Mail, and in Mozilla Thunderbird*. **Shadowing: Outgoing Messages, Outgoing Files** – Enables shadow copying of sent e-mail messages with or without attachments. *Shadow copies of sent e-mail messages with or without attachments are written to the log as .eml files. You can, for example, open .eml files in Microsoft Outlook Express, in Windows Mail, and in Mozilla Thunderbird*. *The number of attachments is always written to the Shadow Log*. **Note:** When you try to open an .eml file from the Shadow Log, you may experience the following issue: You cannot open an .eml file using Outlook 2007. To resolve this issue, visit the following Web site: http://support.microsoft.com/kb/956693/en-us.
Skype	**Audit: Connection** – Enables audit logging of user attempts to sign in to a Skype account. *The Connection action is written to the log*. **Audit: Incoming Calls** - Enables audit logging of user attempts to receive calls. *The Incoming Call action and Skype names of all call participants are written to the log. The Skype name of the local participant precedes the Skype name of a remote participant*. **Audit: Incoming Messages** – Enables audit logging of user attempts to receive instant messages. *The Chat action and Skype names of all IM participants are written to the log. The Skype name of the local participant precedes the Skype name of a remote participant*. **Audit: Incoming Files** - Enables audit logging of user attempts to receive a file. *The Incoming File action and the name of the file are written to the log*. **Audit: Outgoing Calls** - Enables audit logging of user attempts to make calls. *The Outgoing Call action and Skype names of all call participants are written to the log. The Skype name of the local participant precedes the Skype name of a remote participant*. **Audit: Outgoing Messages** - Enables audit logging of user attempts to send instant messages. *The Chat action and Skype names of all IM participants are written to the log*. **Audit: Outgoing Files** – Enables audit logging of user attempts to send a file. *The Outgoing File action and the name of the file are written to the log*. **Shadowing: Incoming Messages** - Enables shadow copying of received instant messages.

PROTOCOL	AUDIT/SHADOWING RIGHTS
	Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user signs out of Skype. It contains an exact record of all received messages. **Shadowing: Incoming Files** – Enables shadow copying of received files. *Shadow copies of received files are written to the log*. **Shadowing: Outgoing Messages** - Enables shadow copying of sent instant messages. *Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user signs out of Skype. It contains an exact record of all sent messages*. **Shadowing: Outgoing Files** – Enables shadow copying of sent files. *Shadow copies of sent files are written to the log*.
SMB	**Audit: Connection** – Enables audit logging of user attempts to access a shared resource on an SMB server. Also, it enables audit logging of attempts from external computers to access a local shared resource on the computer where DeviceLock Service runs. *The Connection action and the hostname or IP address of the SMB server are written to the log.* **Audit: Incoming Files** – Enables audit logging of user attempts to download a file from an SMB server. Also, it enables audit logging of attempts from external computers to upload a file to a local shared resource on the computer where DeviceLock Service runs. *The Incoming File action and the full name of the file (including the path and file name extension) are written to the log.* **Audit: Outgoing Files** – Enables audit logging of user attempts to upload a file to an SMB server. Also, it enables audit logging of attempts from external computers to download a file from a local shared resource on the computer where DeviceLock Service runs. *The Outgoing File action and the name of the file are written to the log.* **Shadowing: Incoming Files** – Enables shadow copying of files downloaded from an SMB server. Also, it enables shadow copying of files uploaded from external computers to a local shared resource on the computer where DeviceLock Service runs. *Shadow copies of downloaded files are written to the log.* **Shadowing: Outgoing Files** – Enables shadow copying of files uploaded to an SMB server. Also, it enables shadow copying of files downloaded to external computers from a local shared resource on the computer where DeviceLock Service runs. *Shadow copies of uploaded files are written to the log.*
SMTP	**Audit: Connection** – Enables audit logging of user attempts to connect to an SMTP server. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name*

PROTOCOL	AUDIT/SHADOWING RIGHTS
	resolution fails, the host name is not written to the log. **Audit: Outgoing Messages**, **Outgoing Files** – Enables audit logging of user attempts to send an e-mail message with or without attachments. *The Outgoing Message action, the number of attachments, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender=>recipient1, recipient2)*. *The number of attachments is written to the Audit Log only when a Content-Aware Rule for the protocol was used to inspect the e-mail message.* **Shadowing: Outgoing Messages**, **Outgoing Files** – Enables shadow copying of sent e-mail messages with or without attachments. *Shadow copies of sent e-mail messages with or without attachments are written to the log as .eml files. You can, for example, open .eml files in Microsoft Outlook Express, in Windows Mail, and in Mozilla Thunderbird*. *The number of attachments is always written to the Shadow Log*.
Social Networks	**Audit: Connection** – Enables audit logging of user attempts to connect to a social networking site. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log*. **Audit: Outgoing Messages** – Enables audit logging of user attempts to send messages, comments, posts, etc. *The Outgoing Message action and the following information (<site_name>:<content_name>_<Recipient ID>) are written to the log. Recipient IDs are written to the log only if users attempt to send messages. Recipient IDs are written in a number format.* **Audit: Outgoing Files** – Enables audit logging of user attempts to upload media and file content to a social networking site. *The Outgoing File action and the following information (<site_name>:<file_name>) are written to the log*. **Shadowing: Outgoing Messages** – Enables shadow copying of sent messages, comments, posts, etc. *Shadow copies of sent messages, comments, etc. are written to the log*. **Shadowing: Outgoing Files** – Enables shadow copying of files uploaded to a social networking site. *Shadow copies of uploaded files are written to the log*.
Telnet	**Audit: Connection** – Enables audit logging of user attempts to connect to a Telnet site. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*
Torrent	**Audit: Connection** – Enables audit logging of the initial user attempt to connect to a remote host over the protocol. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name*

PROTOCOL	AUDIT/SHADOWING RIGHTS
	resolution fails, the host name is not written to the log.
Web Mail	**Audit: Connection** – Enables audit logging of user attempts to access Webmail. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log*. **Audit: Outgoing Messages**, **Outgoing Files** – Enables audit logging of user attempts to send an e-mail message with or without attachments. *The Outgoing Message action, the name of the e-mail provider (such as Yahoo, Gmail, Hotmail (Outlook.com), etc.), the number of attachments, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender=>recipient1, recipient2)*. *The number of attachments is written to the Audit Log only when a Content-Aware Rule for the protocol was used to inspect the e-mail message.* **Shadowing: Outgoing Messages**, **Outgoing Files** – Enables shadow copying of sent e-mail messages with or without attachments. *Shadow copies of sent e-mail messages with or without attachments are written to the log as .eml files. You can, for example, open .eml files in Microsoft Outlook Express, in Windows Mail, and in Mozilla Thunderbird*. *The number of attachments is always written to the Shadow Log*. **Note:** Webmail services automatically save drafts of messages. DeviceLock handles saving a draft as sending a message.
WhatsApp Web	**Audit: Connection** – Enables audit logging of user attempts to connect to WhatsApp Web host. **Note:** Log records generation threshold is 15 minutes for events from the same user or a process. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*
Windows Messenger	**Audit: Connection** – Enables audit logging of user attempts to connect to the Windows Messenger server. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log*. **Audit: Incoming Messages**, **Outgoing Messages** – Enables audit logging of user attempts to send and receive instant messages. *The Chat action, the ID of the local participant, the IP address with the port number and the name of the host are written to the log*. **Audit: Incoming Files** - Enables audit logging of user attempts to receive a file. *The Incoming File action and the name of the file are written to the log*. **Audit: Outgoing Files** - Enables audit logging of user attempts to send a file.

PROTOCOL	AUDIT/SHADOWING RIGHTS
	The Outgoing File action and the name of the file are written to the log. **Shadowing: Incoming Messages** – Enables shadow copying of received instant messages. *Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all received messages.* **Shadowing: Incoming Files** – Enables shadow copying of received files. *Shadow copies of received files are written to the log*. **Shadowing: Outgoing Messages** – Enables shadow copying of sent instant messages. *Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all sent messages*. **Shadowing: Outgoing Files** – Enables shadow copying of sent files. *Shadow copies of sent files are written to the log*.
Yahoo Messenger	**Audit: Connection** – Enables audit logging of user attempts to connect to the Yahoo Messenger server. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log*. **Audit: Incoming Messages**, **Outgoing Messages** – Enables audit logging of user attempts to send and receive instant messages. *The Chat action, IDs of all IM participants, the IP address with the port number and the name of the host are written to the log. The ID of the local participant precedes the ID of a remote participant*. **Audit: Incoming Files** - Enables audit logging of user attempts to receive a file. *The Incoming File action and the name of the file are written to the log*. **Audit: Outgoing Files** - Enables audit logging of user attempts to send a file. *The Outgoing File action and the name of the file are written to the log*. **Shadowing: Incoming Messages** – Enables shadow copying of received instant messages. *Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all received messages.* **Shadowing: Incoming Files** – Enables shadow copying of received files. *Shadow copies of received files are written to the log*. **Shadowing: Outgoing Messages** – Enables shadow copying of sent instant messages. *Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that*

PROTOCOL	AUDIT/SHADOWING RIGHTS
	is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all sent messages. **Shadowing: Outgoing Files** – Enables shadow copying of sent files. *Shadow copies of sent files are written to the log*.

Note: You can define different online vs. offline audit and shadowing rules for the same user or sets of users. Online audit and shadowing rules (Regular Profile) apply to client computers that are working online. Offline audit and shadowing rules (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define offline audit and shadowing rules for protocols, see "Managing Offline Audit, Shadowing and Alerts for Protocols."

You can define the default audit and shadowing rules for protocols for both types of profiles (Regular Profile and Offline Profile). The default rules apply to the Users and Everyone groups. The following table lists rights granted to these groups by default.

GROUP/ PROTOCOL	USERS	EVERYONE
File Sharing	Audit: Connection Audit: Incoming Files Audit: POST Requests Audit: Outgoing Files	Audit: Connection Audit: Incoming Files Audit: POST Requests Audit: Outgoing Files
FTP	Audit: Connection Audit: Incoming Files Audit: Outgoing Files	Audit: Connection Audit: Incoming Files Audit: Outgoing Files
HTTP	Audit: Connection Audit: Incoming Data Audit: Incoming Files Audit: Outgoing Data Audit: POST Requests Audit: Outgoing Files	Audit: Connection Audit: Incoming Data Audit: Incoming Files Audit: Outgoing Data Audit: POST Requests Audit: Outgoing Files
IBM Notes	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files
ICQ/AOL Messenger	Audit: Connection	Audit: Connection

GROUP/ PROTOCOL	USERS	EVERYONE
	Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files	Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files
IRC	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files
Jabber	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files
Mail.ru Agent	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files
MAPI	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files
Skype	Audit: Connection Audit: Incoming Calls Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Calls Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Incoming Calls Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Calls Audit: Outgoing Messages Audit: Outgoing Files
SMB	Audit: Connection Audit: Incoming Files Audit: Outgoing Files	Audit: Connection Audit: Incoming Files Audit: Outgoing Files

GROUP/ PROTOCOL	USERS	EVERYONE
SMTP	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files
Social Networks	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files
Telnet	Audit: Connection	Audit: Connection
Torrent	Audit: Connection	Audit: Connection
Web Mail	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files
WhatsApp Web	Audit: Connection	Audit: Connection
Windows Messenger	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files
Yahoo Messenger	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Incoming Messages Audit: Incoming Files Audit: Outgoing Messages Audit: Outgoing Files

Managing online (regular) audit, shadowing rules and alerts for protocols involves the following tasks:

- Defining and editing audit and shadowing rules.
- Enabling alerts.
- Undefining audit and shadowing rules.

Online audit, shadowing rules and alerts for a protocol can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that audit, shadowing rules and alerts are not defined for a protocol.

Configured	Indicates that audit, shadowing rules and alerts are defined for a protocol.
No Audit	Indicates one of the following: • Audit rights are not set for all of the users and groups specified in audit and shadowing rules for a protocol. • All users and groups specified in audit and shadowing rules for a protocol are removed. • The Everyone account has no Audit and Shadowing rights and is the only account specified in audit and shadowing rules for a protocol.

Defining and Editing Audit and Shadowing Rules

To define and edit audit and shadowing rules

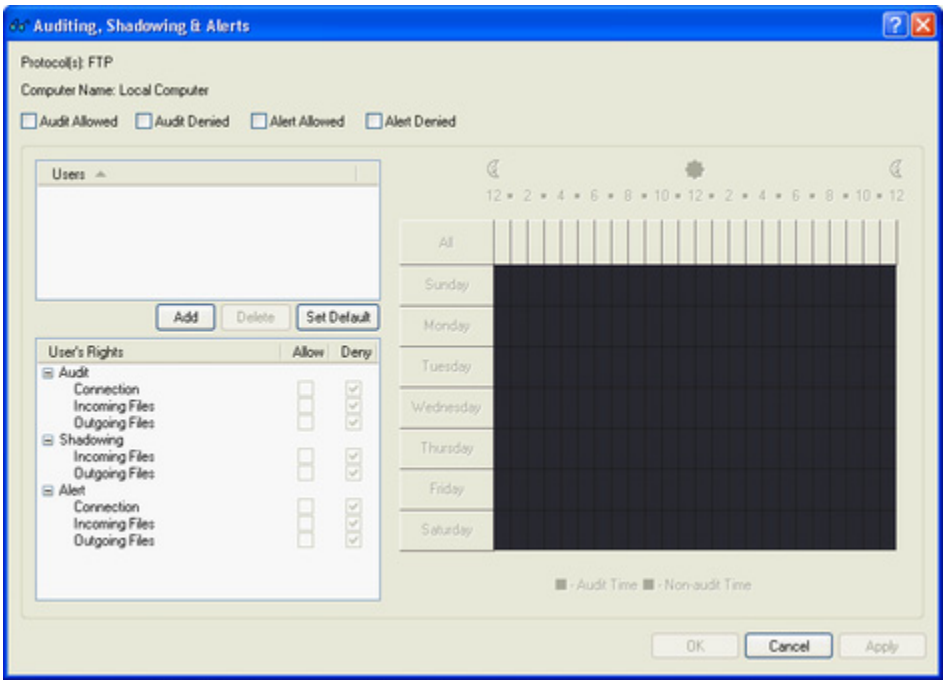
1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Auditing, Shadowing & Alerts**.

   When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view protocols for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of online rules for each protocol in the Regular column.
4. In the details pane, do one of the following:
   - Right-click the protocol for which you want to define or edit rules, and then click **Set Auditing, Shadowing & Alerts**.
     - OR -
   - Select the protocol for which you want to define or edit rules, and then click **Set Auditing, Shadowing & Alerts** on the toolbar.
     - OR -
   - Double-click the protocol for which you want to define or edit rules.

The Auditing, Shadowing & Alerts dialog box appears.



5. In the **Auditing, Shadowing & Alerts** dialog box, do the following:

TO DO THIS	FOLLOW THESE STEPS
To define the default audit and shadowing rules	1. In the upper-left area of the dialog box, specify which events are written to the Audit Log. Select the **Audit Allowed** check box to audit successful attempts to gain access to a protocol. Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a protocol. 2. In the upper-left pane of the dialog box, under **Users**, click **Set Default**. *The default audit and shadowing rules apply to the Users and Everyone groups. For information about which Audit and Shadowing rights are set for these accounts by default, see* "Managing Audit, Shadowing and Alerts for Protocols."
To define audit and shadowing rules for an additional user or group	1. In the upper-left area of the dialog box, specify which events are written to the audit log. Select the **Audit Allowed** check box to audit successful attempts to gain access to a protocol. Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a protocol. 2. In the upper-left pane of the dialog box, under **Users**, click **Add**. *The Select Users or Groups dialog box appears*. 3. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**. *The users and groups that you added are displayed under Users in the upper-left pane of the Auditing, Shadowing & Alerts dialog box*.

TO DO THIS	FOLLOW THESE STEPS
	4. In the upper-left pane of the **Auditing, Shadowing & Alerts** dialog box, under **Users**, select the user or group. *You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them*. 5. In the lower-left pane of the **Auditing, Shadowing & Alerts** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate rights. *In the right pane of the Auditing, Shadowing & Alerts dialog box, you can specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the rule for the selected user or group will or will not be active. Use the left mouse button to select days and hours when the rule is active (audit time). Use the right mouse button to mark days and hours when the rule is not active (non-audit time)*.
To change audit and shadowing rules for an existing user or group	1. In the upper-left pane of the dialog box, under **Users**, select the user or group. 2. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate rights.
To remove an existing user or group and rules	• In the upper-left pane of the dialog box, under **Users,** select the user or group, and then click **Delete** or press the DELETE key. *When you remove a user or group, any rules for that user or group will also be removed*.

6. Click **OK** or **Apply**.

Enabling Alerts

You can enable alerts that are sent when a specific user attempts to access a specific protocol.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for specific events, you must configure alert settings in **Service Options**.

Alerts for specific access-related events are enabled in the **Auditing, Shadowing & Alerts** dialog box. Enabling alerts is similar to defining audit rules and includes the following basic steps:

- Specify which events will trigger alert notifications. You can enable notification of successful and/ or failed attempts to access a protocol. Select the **Alert Allowed** check box to enable notification of successful attempts to access a protocol. Select the **Alert Denied** check box to enable notification of failed attempts to access a protocol.
- Specify users and/or groups whose actions will trigger alert notifications. To do so, in the upper-left pane of the dialog box, under **Users**, click **Add**. In the **Select Users**

or Groups dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.

- Specify which user's actions on protocols either will or will not trigger alert notifications. In the upper-left pane of the dialog box, under **Users**, select the user or group that you added. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny an alert right. Alert rights determine which user actions on protocols trigger alert notifications. Alert rights are identical to audit rights. The only difference is that when events matching specific criteria occur DeviceLock triggers alerts instead of logging these events in the Audit Log. For detailed information on Audit rights for protocols, see the description of rights earlier in this section.
- Specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on protocols either will or will not trigger alert notifications. To do so, in the right pane of the dialog box, use the left mouse button to select days and hours when the selected user's actions on protocols will trigger alert notifications. Use the right mouse button to mark days and hours when the selected user's actions on protocols will not trigger alert notifications.

Note: You can enable different online vs. offline protocol-specific alerts. Online alerts (Regular Profile) are generated when client computers are working online. Offline alerts (Offline Profile) are generated when client computers are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to enable offline alerts, see "Managing Offline Audit, Shadowing and Alerts for Protocols."

Undefining Audit and Shadowing Rules

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent audit and shadowing rules defined for a particular protocol or protocols from being applied to a specific group of client computers. To do so, you need to return the previously defined rules to the unconfigured state. All undefined DeviceLock settings are ignored by client computers.

To undefine audit and shadowing rules

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuratio**n, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Auditing, Shadowing & Alerts**.

When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view protocols for which you can define audit and shadowing rules.

4. In the details pane, right-click the protocol whose rules you want to undefine, and then click **Undefine**.

   You can undefine rules for multiple protocols at the same time. To do this, do the following:

   a) In the details pane, select multiple protocols by holding down the SHIFT key or the CTRL key while clicking them.
   b) Right-click the selection, and then click **Undefine**.

Managing Protocols White List

The Protocols White List lets you selectively allow network communication over any supported protocol regardless of existing protocol blocking settings. The white list is most effective in "least privilege" scenarios when you block all protocol traffic and then specifically authorize only what is required for employees to perform their daily job duties.

For example, suppose that you deny all users access to the SMTP and Web Mail protocols, and then use the white list to let certain users send mail to specific e-mail addresses so that the users can perform their job tasks. By applying these security policies, you can minimize potential risks of data leakage, theft, and misuse.

Note: Shadow copying is not performed for data transfers allowed by the Protocols White List.

The white list consists of rules associated with the specified protocol. Each rule specifies users or groups the rule applies to and contains a set of parameters associated with it.

These parameters fall into two categories:

- General parameters that apply to all protocols.
- Protocol-specific parameters.

The following table describes general parameters for a white list rule.

PARAMETER	DESCRIPTION
Protocol	Specifies the protocol the rule applies to. The following protocols are supported: "Any", File Sharing, FTP, HTTP, IBM Notes, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, MAPI, Skype, SMB, SMTP, Social Networks, SSL, Telnet, Web Mail, Windows Messenger, and Yahoo Messenger. With a white list rule created for the "Any" protocol, you can allow client connections to the specified hosts and/or ports, regardless of the protocol used to establish connections. **Note:** Connections allowed by a white list rule created for the "Any" protocol cannot be blocked by Basic IP Firewall rules.

Name	Specifies the name of the rule.

The following table describes protocol-specific parameters for a white list rule.

PARAMETER	DESCRIPTION
Content Inspection	Applies to all protocols except "Any", SSL, Telnet, and SMB. Specifies whether to enable content inspection for the white listed connection according to defined Content-Aware Rules. If this flag is disabled or no Content-Aware Rule is defined for this connection then content inspection is not performed.
If this rule triggers	Applies to all protocols. Specifies the following additional actions to be performed when the rule triggers: • **Send Alert:** Specifies that an alert is sent whenever the rule triggers. DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific white list rule, you must configure alert settings in **Service Options**. • **Log Event:** Specifies that an event is logged in the Audit Log whenever the rule triggers. The Audit Log Viewer displays the following information about the event: • Type – **Success**. • Date/Time – the date and time when the connection was started in the following format *dd.mm.yyyy hh:mm:ss*, for example, **05.06.2012 14:54:46**. • Source – the type of the protocol involved. • Action - the user's activity type: either **Incoming Connection** or **Outgoing Connection**. • Name – contains no information. • Information - the IP address with the port number and the fully qualified domain name (FQDN) of the remote host, for example, **Remote host: 192.168.100.10:99 (mycomputer.mygroup.mydomain.com)**. • Reason - the cause of the event: **White List: "rule_name"**. • User – the name of the user associated with this event in the following format: <*domain*>\<*username*>. • PID - the identifier of the process associated with this event, for example, **4420**. • Process – the fully qualified path to the process executable file, for example, **C:\Program Files\AppFolder\AppName.exe**.
Hosts:	Applies to the "Any", FTP, HTTP, IBM Notes, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, MAPI, SMB, SMTP, SSL, Telnet, Windows Messenger, and Yahoo Messenger protocols. Specifies a list of allowed hosts for this rule. If this list is specified, these hosts will not be blocked.

PARAMETER	DESCRIPTION
	Hosts may be specified in any of the following formats: • DNS name (for example, **www.example.com**). You can use the asterisk (*) wildcard character in DNS names (for example, ***.example.com** denotes that the host name is any server whose name ends in the specified name). For the HTTP protocol it is possible to allow sub-URLs without allowing the whole URL site (for example, you may allow access only for **www.example.com/section/subsection**). **Caution:** Because DeviceLock uses the local Hosts file for host name resolution, a malicious user with local administrator rights can modify the Hosts file as required to bypass DeviceLock security policies. For example, if the white list allows HTTP access to gmail.com, a malicious user with local administrator rights can gain access to unauthorized www.ru by adding the "**194.87.0.50 gmail.com**" entry to the Hosts file. In order to minimize security risks, we recommend that you secure the Hosts file using the **Prevent Changes In System Configuration Files** option. • IP address (for example, **12.13.14.15**). You can specify a range of IP addresses separated by a dash (-) (for example, **12.13.14.18-12.13.14.28**). You can also specify the subnet mask for the IP address using the following format*: IP address/subnet mask width in bits* (for example, **3.4.5.6/16**). Multiple hosts must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry. You can specify multiple hosts in different formats described above (for example, **www.microsoft.com; 12.13.14.15, 12.13.14.18-12.13.14.28**). **Note:** When adding hosts to the white list, consider the following: If objects (images, scripts, video, Flash files, ActiveX, etc.) on a web page are downloaded from other hosts, you must add those hosts to the white list to load the web page correctly. If you specify hosts and do not specify ports, the hosts can be accessed through all available ports. An application with an embedded SSL certificate (for example, Dropbox, Yandex.Disk, Google Drive, iTunes Google contacts synchronization module, etc.) will fail to connect to its server when the NetworkLock module is active. The NetworkLock module becomes active when you define settings for protocols. To solve this issue, add the server host to the white list for SSL. You can use TcpView to look up the server host. Whitelisting a server host causes all SSL traffic between an application and the specified server host to bypass access control, audit, shadow copying and content filtering. When Outlook starts it connects to both the Exchange server and domain controller. If you set the No Access permission for the MAPI protocol and then add a MAPI white list rule, you must specify the host name of your Exchange server and the host name of the domain controller to avoid connection problems. Same applies to IBM Notes client, IBM Domino server and the names of the

PARAMETER	DESCRIPTION
	corresponding domain controllers.
Ports:	Applies to the "Any", FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, SMTP, SSL, Telnet, Windows Messenger, and Yahoo Messenger protocols. Specifies the port or ports to open for this rule. If this list is specified, these ports will not be blocked. You can specify either a single port or an inclusive range of ports separated by a dash (-). For example, to open port 25, specify **25**. To open ports 5000 to 5020 inclusive, specify **5000-5020**. Multiple ports or port ranges must be separated by a comma (,) or semicolon (;). For example, **25, 36; 8080, 5000-5020**. You can also press ENTER after each entry. **Note:** If you specify ports and do not specify hosts, users can access all hosts available through the specified ports.
File Sharing Services	Applies to the File Sharing protocol. Specifies a list of allowed Web-based file storage, sharing and synchronization services for this rule. If this list is specified, information exchanged via these services will not be blocked. The following Web-based file storage, sharing and synchronization services are supported: Amazon Simple Storage Service (Amazon S3), Dropbox, Box, Google Docs/Google Drive, Rusfolder (Rusfolder.com, former iFolder.ru), OneDrive (former SkyDrive), Yandex.Disk, iCloud and Cloud Mail.ru.
SSL	Applies to the File Sharing, FTP, HTTP, ICQ/AOL Messenger, IRC, SMTP, and Web Mail protocols. Sets the SSL options. The following SSL options are available: • **Allowed** Allows SSL connections. • **Denied** Disallows SSL connections. • **Required** Requires that all connections use SSL.
Local sender ID(s):	Applies to the ICQ/AOL Messenger, Jabber, Mail.ru Agent, Skype, Windows Messenger, and Yahoo Messenger protocols. Specifies a list of identifiers for local users who are allowed to send instant messages or mail. If this list is specified, instant messages or mail from these users will not be blocked. ICQ/AOL Messenger users are identified by numbers called UIN (for example, **111222, 23232323**). Jabber users are identified by Jabber IDs in the following format: **user@example.com**. Mail.ru Agent users are identified by mail.ru e-mail addresses in the following format: **user@mail.ru**. Skype users are identified by Skype names. Windows Messenger users are identified by e-mail addresses in the following format: **user@example.com**. Yahoo Messenger users are identified by any of the following user ID types: • **Yahoo! ID** (<username> or <username>@yahoo.com)

PARAMETER	DESCRIPTION
	• **Rocketmail** (<username>@rocketmail.com) • **Ymail** (<username>@ymail.com) Multiple user identifiers must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry.
Remote recipient ID(s):	Applies to the ICQ/AOL Messenger, Jabber, Mail.ru Agent, Skype, and Yahoo Messenger protocols. Specifies a list of identifiers for remote users who are allowed to receive instant messages or mail. If this list is specified, instant messages or mail to these users will not be blocked. ICQ/AOL Messenger users are identified by numbers called UIN (for example, **111222, 23232323**). Jabber users are identified by Jabber IDs in the following format: **user@example.com**. Mail.ru Agent users are identified by mail.ru e-mail addresses in the following format: **user@mail.ru**. Skype users are identified by Skype names. Windows Messenger users are identified by e-mail addresses in the following format: **user@example.com**. Yahoo Messenger users are identified by any of the following user ID types: • **Yahoo! ID** (<username> or <username>@yahoo.com) • **Rocketmail** (<username>@rocketmail.com) • **Ymail** (<username>@ymail.com) Multiple user identifiers must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry.
Local sender Email(s):	Applies to the IBM Notes, MAPI, SMTP and Web Mail protocols. Specifies a list of allowed e-mail senders for this rule. If this list is specified, mail from these senders will not be blocked. Use the following format for a sender address: *user@domain.com* (*user/domain* for IBM Notes). You can use the asterisk (*) as a wildcard character to specify a group of senders. You can add the asterisk before or after the at sign (@) in an e-mail address. For example, to allow mail delivery from all users in a domain, type ***@domain.com** (***/domain** for IBM Notes)**.** Multiple e-mail addresses must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry. **Note:** When adding senders/recipients to the white list for Web Mail, consider the following: Messages sent from a Webmail application are kept in the Sent Items folder and can be forwarded to any address from any computer.
Remote recipient Email(s):	Applies to the IBM Notes, MAPI, SMTP and Web Mail protocols. Specifies a list of allowed e-mail recipients for this rule. If this list is specified, mail to these recipients will not be blocked. Use the following format for a recipient address: *user@domain.com* (*user/domain*

PARAMETER	DESCRIPTION
	can also be used for IBM Notes). You can use the asterisk (*) as a wildcard character to specify a group of recipients. You can add the asterisk before or after the at sign (@) in an e-mail address. For example, to allow mail delivery to all users in a domain, type ***@domain.com** (***/domain** can also be used for IBM Notes). Multiple e-mail addresses must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry.
Social Networks	Applies to the Social Networks protocol. Specifies a list of allowed social networking sites for this rule. If this list is specified, these social networking sites will not be blocked. The following social networking sites are supported: Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, StudiVZ, Tumblr, Twitter, Vkontakte, XING, Disqus, LiveInternet.ru.
Web Mail Services	Applies to the Web Mail protocol. Specifies a list of allowed Web-based e-mail services for this rule. If this list is specified, e-mail messages sent through these mail services will not be blocked. The following Web-based e-mail services are supported: AOL Mail, Gmail, GMX Mail, Hotmail (Outlook.com), Mail.ru, Outlook Web App (OWA), Rambler Mail, Web.de, Yahoo! Mail, and Yandex Mail.

Note: You can define different online vs. offline Protocols White Lists for the same user or sets of users. The online Protocols White List (Regular Profile) applies to client computers that are working online. The offline Protocols White List (Offline Profile) applies to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define the offline Protocols White List, see "Managing Offline Protocols White List."

Managing the online (regular) Protocols White List involves the following tasks:

- Defining the Protocols White List.
- Editing the Protocols White List.
- Copying rules of the Protocols White List.
- Exporting and importing the Protocols White List.
- Undefining the Protocols White List.
- Deleting rules of the Protocols White List.

Defining Protocols White List

To define the Protocols White List

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

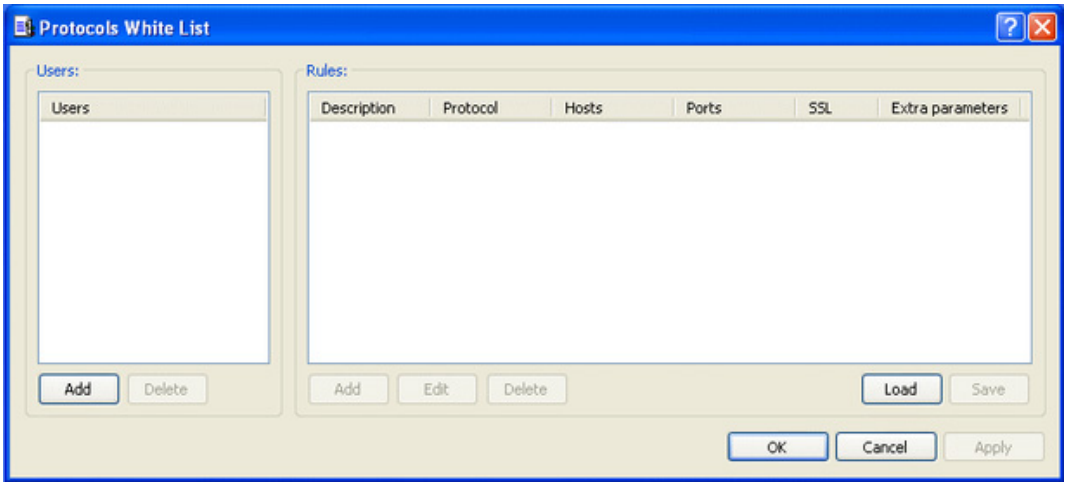
   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **White List**, and then click **Manage**.
     - OR -
   - Select **White List**, and then click **Manage** on the toolbar.

   The Protocols White List dialog box appears.



4. In the left pane of the **Protocols White List** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the Protocols White List, and then click **OK**.

   The users and groups that you added are displayed under Users in the left pane of the Protocols White List dialog box.

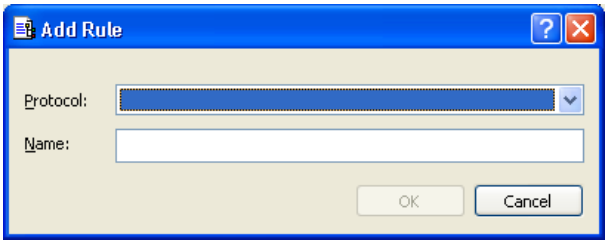
   To delete a user or group, in the left pane of the **Protocols White List** dialog box, under **Users**, select the user or group, and then click **Delete**.

6. In the left pane of the **Protocols White List** dialog box, under **Users**, select the user or group.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

7. In the right pane of the **Protocols White List** dialog box, under **Rules**, click **Add**.

   The Add Rule dialog box appears.



8. In the **Add Rule** dialog box, specify general and protocol-specific parameters for this rule. To specify general parameters, do the following:
   - To specify the protocol, in the **Protocol:** list, click the protocol of your choice.
   - To specify the rule name, in the **Name** box, type a name.

   To specify protocol-specific parameters, do the following:
   - To enable content inspection, click **Content Inspection**. For more information, see the description of the Content Inspection parameter earlier in this section.
   - To specify additional actions to be performed when this rule triggers, click **If this rule triggers**. For more information, see the description of the If this rule triggers parameter earlier in this section.
   - To specify the hosts, in the **Hosts:** box, type host names or IP addresses separated by a comma or semicolon. For more information on how to specify hosts, see the description of the Hosts parameter earlier in this section.
   - To specify the ports, in the **Ports:** box, type port numbers separated by a comma or semicolon. For more information on how to specify ports, see the description of the Ports parameter earlier in this section.
   - To specify the Web-based file storage, sharing and synchronization services, under **File Sharing Services:**, select the appropriate check boxes. For more information, see the description of the File Sharing Services parameter earlier in this section.
   - To configure the SSL options, under **SSL**, click any of the following: **Allowed** (allows SSL connections), **Denied** (disallows SSL connections), or **Required** (requires that all connections use SSL).
   - To specify the IM local sender ID(s), in the **Local sender ID(s):** box, type user identifiers separated by a comma or semicolon. For more information on how to specify user identifiers, see the description of the Local sender ID(s) parameter earlier in this section.
   - To specify the IM remote recipient ID(s), in the **Remote recipient ID(s):** box, type user identifiers separated by a comma or semicolon. For more information on how to specify user identifiers, see the description of the Remote recipient ID(s) parameter earlier in this section.
   - To specify the e-mail senders, in the **Local sender Email(s):** box, type sender addresses separated by a comma or semicolon. For more information on how to specify sender addresses, see the description of the Local sender Email(s): parameter earlier in this section.
   - To specify the e-mail recipients, in the **Remote recipient Email(s):** box, type recipient addresses separated by a comma or semicolon. For more information on how to specify recipient addresses, see the description of the Remote recipient Email(s): parameter earlier in this section.

- To specify the social networking sites, under **Social Networks:**, select the appropriate check boxes. For more information, see the description of the Social Networks: parameter earlier in this section.
- To specify the Web-based e-mail services, under **Web Mail Services:**, select the appropriate check boxes. For more information, see the description of the Web Mail Services: parameter earlier in this section.

9. Click **OK**.

   The rule you created is displayed under Rules in the right pane of the Protocols White List dialog box.

10. Click **OK** or **Apply**.

    The users or groups to which the white list rule applies are displayed under White List in the console tree.

    When you select a user or group to which a white list rule applies in the console tree, in the details pane you can view detailed information regarding this rule. This information includes the following:

    - **Protocol** The protocol the rule applies to.
    - **Name** The name of the rule.
    - **Hosts** Shows the allowed hosts for this rule.
    - **Ports** Shows the allowed ports for this rule.
    - **SSL** Shows the selected SSL option. Possible values: **Allowed** (allows SSL connections), **Denied** (disallows SSL connections), and **Required** (requires that all connections use SSL).
    - **Content Inspection** Shows whether the content inspection is enabled or not.
    - **Extra parameters** Shows additional protocol-specific parameters specified for the rule. These parameters include: **From** (shows allowed sender identifiers for instant messaging and e-mail sender addresses for Webmail) and **To** (shows allowed recipient identifiers for instant messaging and e-mail recipient addresses for Webmail).
    - **Profile** Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to computers that are working offline.
      You can define different online vs. offline Protocols White Lists for the same user or sets of users. For information about how to define the offline Protocols White List, see "Managing Offline Protocols White List."

Editing Protocols White List

You can modify parameter values specified for a white list rule any time you want.

To edit a white list rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.

b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, right-click **White List**, click **Manage**, and then do the following:

a) In the left pane of the **Protocols White List** dialog box, under **Users**, select the user or group for which you want to edit the rule.
By selecting users or groups, you can view the white list rules applied to them under Rules in the right pane of the dialog box.
b) In the right pane of the **Protocols White List** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.
- OR -
Right-click the rule, and then click **Edit**.

- OR -

Under **Protocols**, expand **White List**, and then do the following:

a) Under **White List**, select the user or group for which you want to edit the rule.
By selecting users or groups, you can view the white list rules applied to them in the details pane.
b) In the details pane, right-click the rule you want to edit, and then click **Edit.**
- OR -
In the details pane, double-click the rule you want to edit.

The Edit Rule dialog box appears.

4. In the **Edit Rule** dialog box, modify the rule parameters as required to meet your needs.
5. Click **OK** to apply the changes.

Copying Rules of Protocols White List

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing rules of the Protocols White List.

To copy a white list rule

1. If you use DeviceLock Management Console, do the following:

a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **White List**, and then click **Manage**.
     - OR -
   - Select **White List**, and then click **Manage** on the toolbar.

   The Protocols White List dialog box appears.
4. In the left pane of the **Protocols White List** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.

   By selecting users or groups, you can view the white list rules applied to them under Rules in the right pane of the dialog box.
5. In the right pane of the **Protocols White List** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

   The rule you cut or copy is automatically copied to the Clipboard.

   You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.
6. In the left pane of the **Protocols White List** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.
7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the left pane of the Protocols White List dialog box.
8. In the left pane of the **Protocols White List** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.
9. In the right pane of the **Protocols White List** dialog box, right-click in the **Rules** pane and then click **Paste**.

   The copied rule is displayed under Rules in the right pane of the Protocols White List dialog box.
10. Click **OK** or **Apply** to apply the copied rule.

Exporting and Importing Protocols White List

You can export all your current rules of the Protocols White List to a .pwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

To export the Protocols White List

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **White List**, and then click **Save**.
     - OR -
   - Select **White List**, and then click **Save** on the toolbar.
     - OR -
   - Expand **White List**, right-click any user or group specified in the white list, and then click **Save**.
     - OR -
   - Expand **White List**, select any user or group specified in the white list. In the details pane, right-click the white list rule, and then click **Save**.
     - OR –
   - Expand **White List**, select any user or group specified in the white list, and then click **Save** on the toolbar.
     - OR -
   - Right-click **White List**, and then click **Manage**. In the right pane of the **Protocols White List** dialog box, under **Rules**, click **Save**.

   The Save As dialog box appears.
4. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the .pwl file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.

   When you export the Protocols White List, it is saved in a file with a .pwl extension.

To import the Protocols White List

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

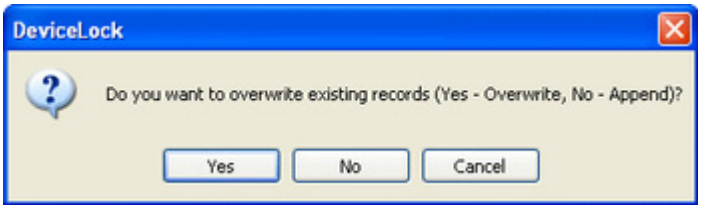
If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **White List**, and then click **Load**.
     - OR -
   - Select **White List**, and then click **Load** on the toolbar.
     - OR -
   - Expand **White List**, right-click any user or group specified in the white list, and then click **Load**.
     - OR -
   - Expand **White List**, select any user or group specified in the white list. In the details pane, right-click the white list rule, and then click **Load**.
     - OR -
   - Expand **White List**, select any user or group specified in the white list, and then click **Load** on the toolbar
     - OR -
   - Right-click **White List**, and then click **Manage**. In the right pane of the **Protocols White List** dialog box, under **Rules**, click **Load**.

   The Open dialog box appears.
4. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
5. In the folder list, locate and open the folder that contains the file.
6. Click the file, and then click **Open**.

   If the Protocols White List is already defined and you choose to import a new white list, the following message box is displayed.



   In the message box, click **Yes** to overwrite the existing white list. Click **No** to append a new white list to the existing white list.

Undefining Protocols White List

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent the Protocols White List from being applied to a specific group of client computers. To do so, you need to return the

previously defined white list to the unconfigured state. All undefined DeviceLock settings are ignored by client computers.

To undefine the Protocols White List

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **White List**, and then click **Undefine**.

Deleting Rules of Protocols White List

You can delete individual white list rules when they are no longer required.

To delete a white list rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Expand **White List**, right-click the user or group to which the rule is applied, and then click **Delete user**.
     When you delete a user or group, the rule associated with this user or group is automatically deleted.

     - OR -
   - Expand **White List**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.
     - OR -

- Right-click **White List**, and then click **Manage**. In the left pane of the **Protocols White List** dialog box, under **Users**, select the user or group to which the rule is applied. In the right pane of the **Protocols White List** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.

Managing Basic IP Firewall

The IP Firewall lets you control network traffic that is not controlled by NetworkLock's list of managed protocols and is not allowed by the Protocols White List, thus increasing security of network communication. You can configure and use the firewall to track TCP and UDP packets, allowing only authorized traffic.

The IP Firewall uses a set of rules that either allow or block traffic over a network connection. Each rule specifies the criteria that a packet must match and the resulting action, either allow or deny, that is taken when a match is found. When a client computer attempts to connect to another computer, the firewall automatically checks all the incoming and outgoing traffic packets against your pre-configured rule set. At the first match, the firewall either allows or denies the packets.

By using firewall rules, you can allow only specific network connections, based on the direction of the traffic, protocol, remote computer address, and destination ports.

There are two basic approaches when configuring the firewall:

- You deny all traffic and create exceptions to explicitly allow a connection through the firewall.
- You block access to specific hosts and/or ports.

The following table describes parameters for a firewall rule. These parameters specify the conditions under which a network connection is allowed or blocked.

PARAMETER	DESCRIPTION
Name	Specifies the name of the firewall rule.
Protocol	Specifies the protocol over which the packet is being transferred. The available options are: **TCP** and **UDP**.
Type	Specifies the action to take with packets that match the specified criteria. It can be one of the following: • **Allow**. The traffic is not secured. It is allowed to be sent and/or received without intervention. • **Deny**. The traffic is blocked. Please note that the traffic is blocked only if the amount of data transferred in either direction (incoming or outgoing) exceeds 8 KB.
Direction	Specifies the direction of traffic to which the rule applies. The available options are: • **Incoming**. The rule applies to incoming traffic.

PARAMETER	DESCRIPTION
	• **Outgoing**. The rule applies to outgoing traffic.
If this rule triggers	Specifies the following additional actions to be performed when the rule triggers: • **Send Alert:** Specifies that an alert is sent whenever the rule triggers. DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific firewall rule, you must configure alert settings in **Service Options**. • **Log Event:** Specifies that an event is logged in the Audit Log whenever the rule triggers. The Audit Log Viewer displays the following information about the event: • Type – the class of an event, either **Success** for traffic allowed by the firewall or **Failure** for traffic denied by the firewall. • Date/Time – the date and time when the event occurred in the following format *dd.mm.yyyy hh:mm:ss*, for example, **05.06.2012 14:54:46**. For the allowed traffic – the date and time when the connection was started. For the denied traffic - the date and time when the packet was dropped. • Source – the type of the protocol involved: **IP**. • Action - the user's activity type: either **Incoming Connection** or **Outgoing Connection**. • Name – contains no information. • Information - the IP address with the port number and the fully qualified domain name (FQDN) of the remote host, for example, **Remote host: 192.168.100.10:99 (mycomputer.mygroup.mydomain.com)**. • Reason - the cause of the event: **IP Firewall: "rule_name"**. • User – the name of the user associated with this event in the following format: *<domain>\<username>*. • PID - the identifier of the process associated with this event, for example, **4420**. • Process – the fully qualified path to the process executable file, for example, **C:\Program Files\AppFolder\AppName.exe**.
Hosts:	Specifies the remote hosts to which the rule applies. The remote hosts are the computers that communicate with client computers running DeviceLock Service. Hosts may be specified in any of the following formats: • DNS name (for example, **www.example.com**). You can use the asterisk (*) wildcard character in DNS names (for example, ***.example.com** denotes that the host name is any server whose name ends in the specified name). • IP address (for example, **12.13.14.15**). You can specify a range of IP addresses separated by a dash (-) (for example, **12.13.14.18-12.13.14.28**). Multiple hosts must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry. You can specify multiple hosts in different formats described above (for example,

PARAMETER	DESCRIPTION
	www.microsoft.com; 12.13.14.15, 12.13.14.18-12.13.14.28). **Note:** If you specify hosts and do not specify ports, the rule will either allow or block all client connections to the specified hosts.
Ports:	Specify the ports on remote hosts to which the rule applies. You can specify either a single port or an inclusive range of ports separated by a dash (-). For example, to open port 110, specify **110**. To open ports 5000 to 5020 inclusive, specify **5000-5020**. Multiple ports or port ranges must be separated by a comma (,) or semicolon (;). For example, **110, 36; 8080, 5000-5020**. You can also press ENTER after each entry. **Note:** If you specify ports and do not specify hosts, the rule will either allow or block all client connections to the specified ports.

When defining firewall rules, consider the following:

- When the Allow and Deny rules are applied in conjunction, all Allow rules override the Deny rules for both incoming and outgoing traffic.
- Firewall rules have a lower priority than settings specified at the protocol level (Permissions, the Protocols White List).
- Some applications, for example, Windows built-in applications (such as Remote Desktop) use system processes to transfer data. To block such applications, you must create and apply a firewall rule to the account that is used by the application's data transfer process.
- When users try to establish a connection to which they are denied access, they receive a Basic IP Firewall blocked message, if Basic IP Firewall blocked message is enabled in Service Options. For detailed information on this message, see "Basic IP Firewall blocked message" in "**Service Options**".
- The communication between DeviceLock Service and DeviceLock Enterprise Server as well as between DeviceLock Service and DeviceLock Management Console is always allowed, regardless of firewall settings.

Note: You can define different online vs. offline firewall rules for the same user or sets of users. Online firewall rules (Regular Profile) apply to client computers that are working online. Offline firewall rules (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define offline firewall rules, see "Managing Offline IP Firewall."

Managing online (regular) firewall rules involves the following tasks:

- Defining firewall rules.
- Editing firewall rules.
- Copying firewall rules.

- Exporting and importing firewall rules.
- Undefining firewall rules.
- Deleting firewall rules.

You can manage firewall rules using DeviceLock Management Console, DeviceLock Group Policy Manager, or DeviceLock Service Settings Editor.

Defining Firewall Rules

You can enable alerts that are sent when a specific firewall rule fires. Such alerts are enabled at the time you define a firewall rule.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific firewall rule, you must configure alert settings in **Service Options**.

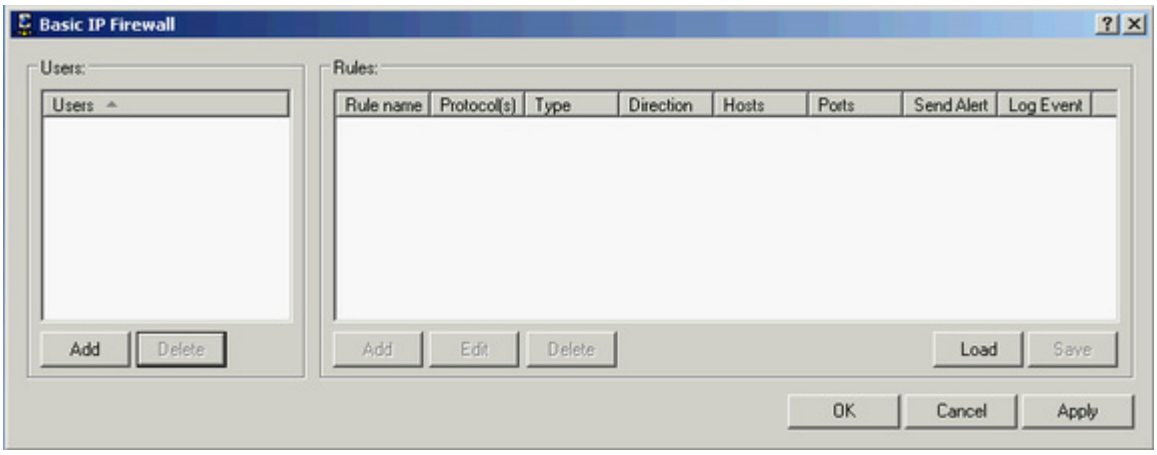
To define a firewall rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Basic IP Firewall**, and then click **Manage**.
     - OR -
   - Select **Basic IP Firewall**, and then click **Manage** on the toolbar.

   The Basic IP Firewall dialog box appears.



4. In the left pane of **the Basic IP Firewall** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the firewall rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the left pane of the Basic IP Firewall dialog box.

   To delete a user or group, in the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user or group, and then click **Delete**.

6. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user or group.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

7. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Add**.

   The Add Rule dialog box appears.

8. In the **Add Rule** dialog box, specify the firewall rule parameters:

   - To specify the rule name, in the **Name** box, type a name.
   - To specify the protocol, under **Protocol**, select the check box next to the protocol of your choice.
   - To specify what actions the firewall takes for all connections that match the rule's criteria, under **Type**, click either of the following options: **Allow** or **Deny**.
   - To specify the direction of traffic to which the rule applies, under **Direction**, select the appropriate check box.
   - To specify additional actions to be performed when the rule triggers, under **If this rule triggers**, select the appropriate check box.
   - To specify the remote hosts to which the rule applies, in the **Hosts:** box, type host names or IP addresses separated by a comma or semicolon.
   - To specify the ports on remote hosts to which the rule applies, in **the Ports:** box, type port numbers separated by a comma or semicolon.

   For more information, see the description of the firewall rule parameters earlier in this section.

9. Click **OK**.

   The rule you created is displayed under Rules in the right pane of the Basic IP Firewall dialog box.

10. Click **OK** or **Apply**.

    The users or groups to which the firewall rule applies are displayed under Basic IP Firewall in the console tree.

    When you select a user or group to which a firewall rule applies in the console tree, in the details pane you can view detailed information regarding this rule. This information includes the following:

    - **Name** The name of the rule.
    - **Protocol(s)** The protocol(s) to which the rule applies: **TCP** and/or **UDP**.

- **Type** The action the firewall takes for all connections that match the rule's criteria. Possible actions: **Allow** (allows the connection) and **Deny** (blocks the connection).
- **Direction** The direction of traffic to which the rule applies: **Incoming** and/or **Outgoing**.
- **Hosts** Shows the specified hosts for this rule.
- **Ports** Shows the specified ports for this rule.
- **Send Alert** Shows whether alerts are enabled or disabled for this rule.
- **Log Event** Shows whether audit logging of events associated with this rule is enabled or disabled.
- **Profile** Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to client computers that are working offline.

  You can define different online vs. offline firewall rules for the same user or sets of users. For information about how to define offline firewall rules, see "Managing Offline IP Firewall."

Editing Firewall Rules

You can modify parameter values specified for a firewall rule any time you want.

To edit a firewall rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined online (regular) DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Basic IP Firewall**, click **Manage**, and then do the following:
   a) In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user or group for which you want to edit the rule.
   By selecting users or groups, you can view the firewall rules applied to them under Rules in the right pane of the dialog box.
   b) In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.
   - OR -

Right-click the rule, and then click **Edit**.

- OR -

Under **Protocols**, expand **Basic IP Firewall**, and then do the following:

a) Under **Basic IP Firewall**, select the user or group for which you want to edit the rule.

By selecting users or groups, you can view the firewall rules applied to them in the details pane.

b) In the details pane, right-click the rule you want to edit, and then click **Edit**.

- OR -

In the details pane, double-click the rule you want to edit.

The Edit Rule dialog box appears.

4. In the **Edit Rule** dialog box, modify the rule parameters as required to meet your needs.
5. Click **OK** to apply the changes.

Copying Firewall Rules

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing firewall rules.

To copy a firewall rule

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined online (regular) DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

   - Right-click **Basic IP Firewall**, and then click **Manage**.

     - OR -

   - Select **Basic IP Firewall**, and then click **Manage** on the toolbar.

   The Basic IP Firewall dialog box appears.

4. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.

By selecting users or groups, you can view the firewall rules applied to them under Rules in the right pane of the dialog box.

5. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

   The rule you cut or copy is automatically copied to the Clipboard.

   You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.

   You can copy and then paste several rules at the same time. Hold down the SHIFT key or the CTRL key while you click each rule, right-click one of them, and then click **Copy**.

6. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the left pane of the Basic IP Firewall dialog box.

8. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

9. In the right pane of the **Basic IP Firewall** dialog box, right-click in the **Rules** pane and then click **Paste**.

   The copied rule is displayed under Rules in the right pane of the Basic IP Firewall dialog box.

10. Click **OK** or **Apply** to apply the copied rule.

Exporting and Importing Firewall Rules

You can export all your current firewall rules to an .ipp file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

To export firewall rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined online (regular) DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

- Right-click **Basic IP Firewall**, and then click **Save**.
  - OR -
- Select **Basic IP Firewall**, and then click **Save** on the toolbar.
  - OR -
- Expand **Basic IP Firewall**, right-click any user or group specified in the firewall rule, and then click **Save**.
  - OR -
- Expand **Basic IP Firewall**, select any user or group specified in the firewall rule. In the details pane, right-click the firewall rule, and then click **Save**.
  - OR –
- Expand **Basic IP Firewall**, select any user or group specified in the firewall rule, and then click **Save** on the toolbar.
  - OR -
- Right-click **Basic IP Firewall**, and then click **Manage**. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Save**.

The Save As dialog box appears.

4. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the .ipp file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.

When you export firewall rules, they are saved in a file with an .ipp extension.

To import firewall rules

1. If you use DeviceLock Management Console, do the following:

a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

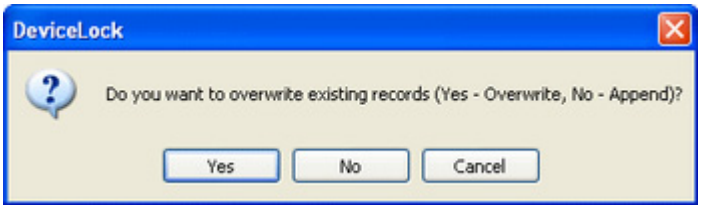
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

- Right-click **Basic IP Firewall**, and then click **Load**.
  - OR -
- Select **Basic IP Firewall**, and then click **Load** on the toolbar.
  - OR -
- Expand **Basic IP Firewall**, right-click any user or group specified in the firewall rule, and then click **Load**.
  - OR -
- Expand **Basic IP Firewall**, select any user or group specified in the firewall rule. In the details pane, right-click the firewall rule, and then click **Load**.
  - OR -
- Expand **Basic IP Firewall**, select any user or group specified in the firewall rule, and then click **Load** on the toolbar.
  - OR -
- Right-click **Basic IP Firewall**, and then click **Manage**. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Load**.

The Open dialog box appears.

4. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
5. In the folder list, locate and open the folder that contains the file.
6. Click the file, and then click **Open**.

   If firewall rules are already defined and you choose to import new firewall rules, the following message box is displayed.



   In the message box, click **Yes** to overwrite the existing firewall rules. Click **No** to append new firewall rules to the existing firewall rules.

Undefining Firewall Rules

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent firewall rules from being applied to a specific group of client computers. To do so, you need to return the previously defined firewall rules to the unconfigured state. All undefined DeviceLock settings are ignored by client computers.

To undefine firewall rules

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined online (regular) DeviceLock policies.

c) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Undefine**.

Deleting Firewall Rules

You can delete individual firewall rules when they are no longer required.

To delete a firewall rule

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined online (regular) DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

   - Expand **Basic IP Firewall**, right-click the user or group to which the rule is applied, and then click **Delete user**.
     When you delete a user or group, the rule associated with this user or group is automatically deleted.
     - OR -
   - Expand **Basic IP Firewall**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.
     - OR -
   - Right-click **Basic IP Firewall**, and then click **Manage**. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user or group to which the rule is applied. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.

Managing Security Settings for Protocols

You can define additional security parameters that affect permissions and audit rules for protocols.

DeviceLock supports these additional security parameters:

- **Block unrecognized outgoing SSL traffic** – if enabled, allows DeviceLock Service to audit and block all unrecognized outgoing SSL traffic. Otherwise, even if the protocols are locked, all unrecognized outgoing SSL traffic is not blocked and audit is not performed for it.
- **Block IP addresses in URL** – if enabled, allows DeviceLock Service to block all URLs containing the host IP address when users have "allow access" permissions for a protocol. Use this setting to block access to sites (for example, Facebook) that can be accessed using an IP address. This setting applies to the following protocols: File Sharing, HTTP, Social Networks, and Web Mail. By default, the setting is disabled.

  Audit and shadow copying for URLs containing the host IP address are performed at the HTTP level. If Block IP addresses in URL is disabled but users have "deny access" permissions for a protocol, all URLs containing the host IP address are also blocked.

  Note: If **Block IP addresses in URL** is enabled and specific host IP addresses are allowed by the Protocols White List, these IP addresses will not be blocked. The Protocols White List settings override Security Settings for protocols.
- **Block proxy traffic** – if enabled, allows DeviceLock Service to audit and block all traffic that flows through a proxy server. The following proxy servers are supported: HTTP, SOCKS4, and SOCKS5.
- **Block network if BFE service is stopped (Windows 8 and later)** – if enabled, tells DeviceLock Service to block all network traffic when the Base Filtering Engine system service is stopped. If this parameter is disabled and the Base Filtering Engine system service is stopped, NetworkLock is unable to control the network traffic on Windows 8 and later systems. This parameter is ignored if there is no NetworkLock policy defined.
- **Intercept MS Lync connections** – if enabled, allows DeviceLock Service to intercept the traffic from Microsoft Lync, Office Communicator, and/or Skype for Business.

Note: You can define different online vs. offline Security Settings for the same user or sets of users. Online Security Settings (Regular Profile) apply to client computers that are working online. Offline Security Settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see "DeviceLock Security Policies (Offline Profile)." For information about how to define offline Security Settings, see "Managing Offline Security Settings for Protocols."

Managing online (regular) Security Settings for protocols involves the following tasks:

- Defining and changing Security Settings.
- Undefining Security Settings.

Online Security Settings for protocols can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that Security Settings are not defined for protocols.
Enabled	Indicates that Security Settings are enabled for protocols.
Disabled	Indicates that Security Settings are disabled for protocols.

Defining and Changing Security Settings

To define and change Security Settings

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Select **Security Settings**. In the details pane, right-click the Security Setting, and then click **Enable** or **Disable**.
     When you select Security Settings in the console tree, they are displayed in the details pane.

     - OR-
   - Right-click **Security Settings**, and then click **Manage**. In the **Security Settings** dialog box that opens, select or clear the appropriate check box, and then click **OK**.
     To open the Security Settings dialog box, you can also select Security Settings, and then click Manage *on the toolbar.*

Undefining Security Settings

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent Security Settings

defined for protocols from being applied to a specific group of client computers. To do so, you need to return the previously defined Security Settings to the unconfigured state. All undefined DeviceLock settings are ignored by client computers.

To undefine Security Settings

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Security Settings**.

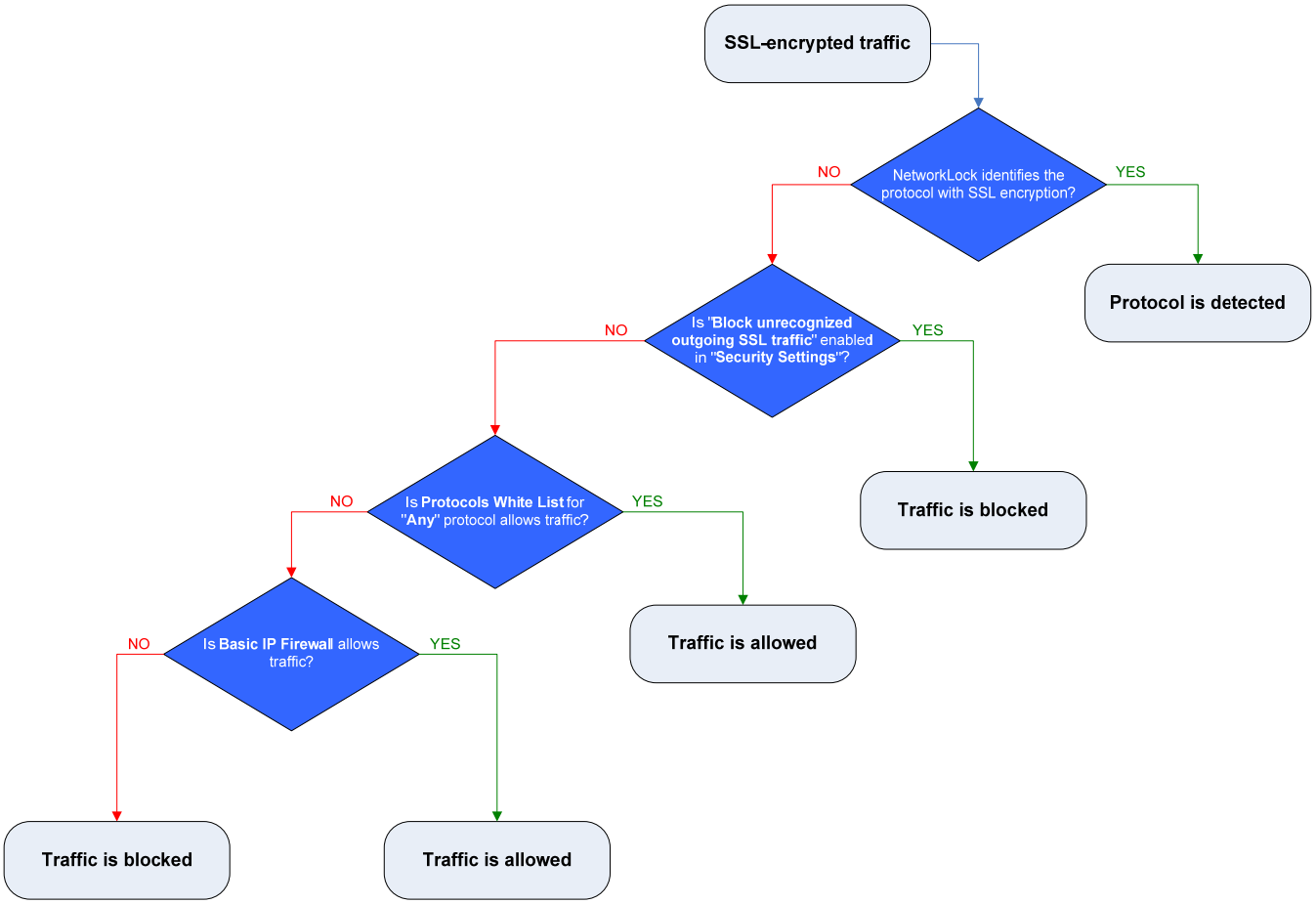
   When you select Security Settings in the console tree, they are displayed in the details pane.
4. In the details pane, right-click the Security Setting you want to undefine, and then click **Undefine**.

Inspection and Control of SSL-encrypted Traffic

Inspection and control of SSL-encrypted traffic includes the following sequential steps:

- Identification of the protocol used with SSL. When the protocol is identified, DeviceLock checks whether the user attempting the connection is allowed to access the connection.
- Checking whether Block unrecognized outgoing SSL traffic is enabled.
- Checking whether traffic is allowed by a white list rule created for "Any" protocol.
- Checking whether traffic is allowed by a firewall rule.

The following illustration shows how DeviceLock inspects SSL-encrypted traffic and applies appropriate security measures based on defined policies.



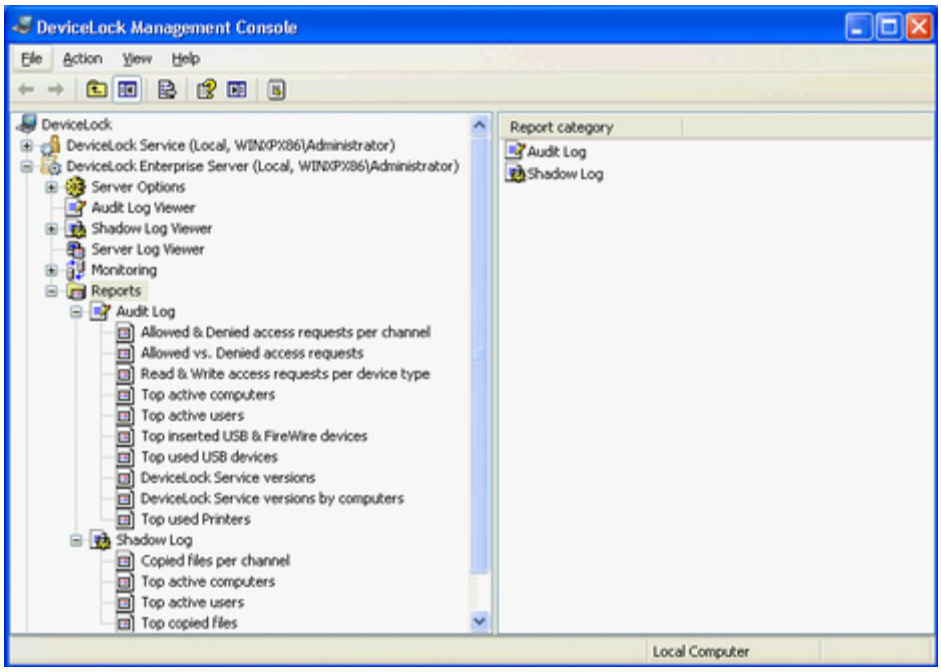
DeviceLock Reports

DeviceLock lets you create reports using data from logs stored on DeviceLock Enterprise Server. Use reports to arrange and display statistical data on a user's device- and protocol-related activities in a separate file. When generating a report, you can define report parameters to filter the data and display the information that is relevant to you. For example, you can specify the start and end date and time of the report period for which data is displayed.

Reports can be created, automatically sent to you via e-mail, stored, exported to a variety of formats and shared with others. Reports are created by using DeviceLock Management Console.

Report Categories and Types

DeviceLock comes with a set of predefined report templates that you can use to create new reports. These predefined templates are displayed in the console tree, under **DeviceLock Enterprise Server**, **Reports**.



Note: You can create only those reports that are based on the predefined templates. You cannot modify the predefined report templates or create your own (custom) report templates.

There are two categories of report templates:

- Audit Log reports
- Shadow Log reports

The report types available in each category are described below.

Audit Log Reports

Audit Log reports are reports that use the DeviceLock Enterprise Server audit log files as a data source. The following table provides summary information on the report types available in this category.

REPORT TYPE	DESCRIPTION
Allowed & Denied access requests per channel	This report shows the number of allowed and denied access requests per data transmission channel (devices and/or protocols). The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **User(s):** Shows the users that were specified for the report. • **Channel(s):** Shows the data transmission channels that were specified for the report. The available options are: **all devices**, **all protocols**, and **all devices and protocols**. **Note:** When **all protocols** or **all devices and protocols** is selected, the report may contain the Other protocol which represent data transmitted via unrecognized protocols logged by Protocols White List (Any and SSL) and Basic IP Firewall rules. The Report Results section contains a table and a chart that show detailed results of the report. The table has the following columns: • **Channel** Shows a data transmission channel. • **Allowed** Shows the number of allowed access requests. • **Denied** Shows the number of denied access requests.
Allowed vs. Denied access requests	This report shows the total number of allowed and denied access requests sent through all data transmission channels (devices and/or protocols). The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very

REPORT TYPE	DESCRIPTION
	beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **User(s):** Shows the users that were specified for the report. • **Channel(s):** Shows the data transmission channels that were specified for the report. The available options are: **all devices**, **all protocols**, and **all devices and protocols**. **Note:** When **all protocols** or **all devices and protocols** is selected, the report may contain data transmitted via unrecognized protocols logged by Protocols White List (Any and SSL) and Basic IP Firewall rules. The Report Results section contains a table and a pie chart that show detailed results of the report. The table has the following rows: • **Allowed** Shows the total number of allowed access requests and the respective percentage. • **Denied** Shows the total number of denied access requests and the respective percentage. • **Total** Shows the total number of all access requests and the respective percentage. The pie chart represents the report results in percentages.
Read & Write access requests per device type	This report shows the number of read and write access requests per device type. The report provides data only for the Floppy, iPhone, MTP, Optical Drive, Removable, TS Devices, Clipboard, Hard disk, Tape, Windows Mobile, and Palm device types. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Access Type(s):** Shows the event types that were specified for the report. • **Computer(s):** Shows the computers that were specified for the report.

REPORT TYPE	DESCRIPTION
	• **User(s):** Shows the users that were specified for the report. The Report Results section contains a table and a chart that show detailed results of the report. The table has the following columns: • **Device Type** Shows a device type. • **Read** Shows the number of read access requests. • **Write** Shows the number of write access requests. The table also has a **Total** row that sums up all the values in the **Read** and **Write** columns.
Top active computers	This report shows the most frequently used computers sorted according to the number of allowed and denied access requests. By default, the report lists the first 10 computers but you can specify any number of computers. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Channel(s):** Shows the device types and/or protocols that were specified for the report. **Note:** You may also select the Other protocol, which represent data transmitted via unrecognized protocols logged by Protocols White List (Any and SSL) and Basic IP Firewall rules. The Report Results section contains two tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) computers having allowed access. Table 2 lists the top N (where N is a specific number) computers having denied access. These tables have the following columns: • **Computer Name** Shows a computer name. • **Access Count** Shows the number of access requests. Values in this column are sorted in descending order.

REPORT TYPE	DESCRIPTION
Top active users	This report shows the most active users sorted according to the number of allowed and denied access requests sent by each user. By default, the report lists the first 10 users but you can specify any number of users. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Channel(s):** Shows the device types and/or protocols that were specified for the report. **Note:** You may also select the Other protocol, which represent data transmitted via unrecognized protocols logged by Protocols White List (Any and SSL) and Basic IP Firewall rules. The Report Results section contains two tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) users having allowed access. Table 2 lists the top N (where N is a specific number) users having denied access. These tables have the following columns: • **User Name** Shows a user name. • **Access Count** Shows the number of access requests. Values in this column are sorted in descending order.

REPORT TYPE	DESCRIPTION
Top inserted USB & FireWire devices	This report shows three groups of the most frequently inserted USB and FireWire devices sorted according to the number of the Insert actions: • Group 1 lists both allowed and denied devices. • Group 2 lists only allowed devices. • Group 3 lists only denied devices. By default, the report lists the first 10 devices in each group but you can specify any number of devices. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Users(s):** Shows the users that were specified for the report. The Report Results section contains three tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) inserted USB & and FireWire devices (both allowed and denied devices). Table 2 lists the top N (where N is a specific number) inserted allowed USB & FireWire devices. Table 3 lists the top N (where N is a specific number) inserted denied USB & FireWire devices. These tables have the following columns: • **Device Name** Shows a device name. • **Insert Count** Shows the number of the Insert actions. Values in this column are sorted in descending order.
Top used USB devices	This report shows three groups of the most frequently used USB devices sorted according to the number of access requests: • Group 1 lists devices having both allowed and denied access. • Group 2 lists devices having only allowed access. • Group 3 lists devices having only denied access. By default, the report lists the first 10 devices in each group but you can specify any number of devices. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type.

REPORT TYPE	DESCRIPTION
	The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Users(s):** Shows the users that were specified for the report. The Report Results section contains three tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) USB devices having both allowed and denied access. Table 2 lists the top N (where N is a specific number) USB devices having allowed access. Table 3 lists the top N (where N is a specific number) USB devices having denied access. These tables have the following columns: • **Device Name** Shows a device name. • **Access Count** Shows the number of access requests. Values in this column are sorted in descending order.
DeviceLock Service versions	This report shows the total number of computers with the specified version(s) of DeviceLock Service and the number of computers that have different build numbers for each version. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running*. • **Computer(s):** Shows the computers that were specified for the report. • **Version(s):** Shows the DeviceLock Service versions that were specified for the report. The Report Results section contains a table and a pie chart that show detailed results of the report. The table has the following columns: • **Version** Shows a version number. • **Build** Shows build numbers of the version. Values in this column are sorted in descending order.

REPORT TYPE	DESCRIPTION
	• **Number of Computers** Shows the number of computers that have a specific build number and the total number of computers with the specified version(s) of DeviceLock Service. The pie chart shows the percentage of computers with the specified version(s) of DeviceLock Service.
DeviceLock Service versions by computers	This report shows the list of specified DeviceLock Service versions and computer names and the total number of computers for each version. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running*. • **Computer(s):** Shows the computers that were specified for the report. • **Version(s):** Shows the DeviceLock Service versions that were specified for the report. The Report Results section contains a table with detailed results of the report. This table has the following columns: • **Version** Shows a version number. • **Computer name** Shows computer names and the total number of computers for each specified version.
DeviceLock policy changes	This report shows the list of policy change events. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running*. • **Computer(s):** Shows the computers that were specified for the report. • **Users(s):** Shows the users that were specified for the report. The Report Results section contains a table with detailed results of the report. This

REPORT TYPE	DESCRIPTION
	table has the following columns: • **Date/time** Shows the date and the time of a policy change event. • **Action** Shows detailed information on policy change event. • **User** Shows the user who modified the policy.
Top used Printers	This report shows three groups of the most frequently used printers sorted according to the number of access requests: • Group 1 lists printers having both allowed and denied access. • Group 2 lists printers having only allowed access. • Group 3 lists printers having only denied access. By default, the report lists the first 10 printers in each group but you can specify any number of printers. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running*. • **Computer(s):** Shows the computers that were specified for the report. • **Users(s):** Shows the users that were specified for the report. The Report Results section contains three tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) printers having both allowed and denied access. Table 2 lists the top N (where N is a specific number) printers having allowed access. Table 3 lists the top N (where N is a specific number) printers having denied access. These tables have the following columns: • **Device Name** Shows a printer name. • **Access Count** Shows the number of access requests. Values in this column are sorted in descending order.

REPORT TYPE	DESCRIPTION
Top active processes	This report shows the most active processes (applications) sorted according to the number of allowed and denied access requests sent by each process. By default, the report lists the first 10 processes but you can specify any number of processes. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Channel(s):** Shows the device types and/or protocols that were specified for the report. **Note:** You may also select the Other protocol, which represent data transmitted via unrecognized protocols logged by Protocols White List (Any and SSL) and Basic IP Firewall rules. The Report Results section contains two tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) processes having allowed access. Table 2 lists the top N (where N is a specific number) processes having denied access. These tables have the following columns: • **Process Name** Shows a process name. • **Access Count** Shows the number of access requests. Values in this column are sorted in descending order.

REPORT TYPE	DESCRIPTION
Top copied files by extension	This report shows three groups of the most frequently copied file extensions sorted according to the number of the read and write actions: • Group 1 lists both allowed and denied actions. • Group 2 lists only allowed actions. • Group 3 lists only denied actions. By default, the report lists the first 10 file extensions in each group but you can specify any number of file extensions. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Users(s):** Shows the users that were specified for the report. • **Channel(s):** Shows the device types and/or protocols that were specified for the report. The Report Results section contains three tables and charts with detailed results of the report. Table 1 lists the top N (where N is a specific number) file extensions (both allowed and denied actions). Table 2 lists the top N (where N is a specific number) file extensions with allowed actions. Table 3 lists the top N (where N is a specific number) file extensions with denied actions. These tables have the following columns: • **Extension** Shows a file extension. • **Read** Shows the number of read actions. • **Write** Shows the number of write actions. The tables also have a **Total** row that sums up all the values in the **Read** and **Write** columns. The **No extension** label is used for all files without an extension, and the **Other** label is used for all file extensions whose combined percentage out of the total number of files is less than 5%. The **Direct access** label is used for all CD/DVD/BD burn and direct-write operations (e.g. formatting).

REPORT TYPE	DESCRIPTION
Top printed documents	This report shows the most frequently printed documents (files) sorted according to the number of allowed and denied access requests: • Group 1 lists both allowed and denied actions. • Group 2 lists only allowed actions. • Group 3 lists only denied actions. By default, the report lists the first 10 documents but you can specify any number of documents. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Users(s):** Shows the users that were specified for the report. • **Printer(s):** Shows the printers that were specified for the report. The Report Results section contains three tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) documents (both allowed and denied actions). Table 2 lists the top N (where N is a specific number) documents with allowed actions. Table 3 lists the top N (where N is a specific number) f documents with denied actions. These tables have the following columns: • **File Name** Shows a document name. • **Access Count** Shows the number of access requests. Values in this column are sorted in descending order.

Shadow Log Reports

Shadow Log reports are reports that use the DeviceLock Enterprise Server shadow log files as a data source. All reports contain the combined data from the shadow log and deleted shadow data log. The following table provides summary information on the report types available in this category.

REPORT TYPE	DESCRIPTION
Copied files per channel	This report shows statistics on copied files per data transmission channel (devices and/or protocols), including e-mail attachments. Statistical information on copied files is sorted according to the number of copied files and total size of all copied files separately for allowed and denied copy operations. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Users(s):** Shows the users that were specified for the report. • **File Name:** Shows the files that were specified for the report. • **Channel(s):** Shows the data transmission channels that were specified for the report. The available options are: **all devices**, **all protocols**, and **all devices and protocols**. The Report Results section contains four tables and four pie charts that show detailed results of the report. Table 1 shows the number of copied files for each data transmission channel for allowed copy operations. Table 2 shows the number of copied files for each data transmission channel for denied copy operations. Tables 1 and 2 have the following columns: • **Channel** Shows a data transmission channel. • **Number of Files** Shows the number of copied files. Tables 1 and 2 also have a **Total** row that sums up all the values in the **Number of Files** column. Table 3 shows the total size of copied files for each data transmission channel for allowed copy operations. Table 4 shows the total size of copied files for each data transmission channel for denied copy operations. Tables 3 and 4 have the following columns: • **Channel** Shows a data transmission channel. • **Data Size** Shows the total size of all copied files.

REPORT TYPE	DESCRIPTION
	Tables 3 and 4 also have a **Total** row that sums up all the values in the **Data Size** column. Each table is followed by a pie chart which represents the report results in percentages.
Top active computers	This report shows the most frequently used computers sorted according to the number of copied files and total size of all copied files. By default, the report lists the first 10 computers but you can specify any number of computers. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Channel(s):** Shows the device types and/or protocols that were specified for the report. • **File Name:** Shows the files that were specified for the report. The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) computers having both allowed and denied access by the number of copied files. Table 2 lists the top N (where N is a specific number) computers having both allowed and denied access by the amount of copied data. Table 3 lists the top N (where N is a specific number) computers having allowed access by the number of copied files. Table 4 lists the top N (where N is a specific number) computers having allowed access by the amount of copied data. Table 5 lists the top N (where N is a specific number) computers having denied access by the number of copied files. Table 6 lists the top N (where N is a specific number) computers having denied access by the amount of copied data. Tables 1, 3 and 5 have the following columns: • **Computer Name** Shows a computer name. • **Access Count** Shows the number of access requests. Values in this column are sorted in descending order. Tables 2, 4 and 6 have the following columns: • **Computer Name** Shows a computer name. • **Data Size** Shows the total size of all copied files. Values in this column are sorted in descending order.
Top active users	This report shows the most active users sorted according to the number of copied files and total size of all copied files. By default, the report lists the first 10 users but you can specify any number of users. The report consists of three sections: the Report Header, Report Parameters, and Report Results.

REPORT TYPE	DESCRIPTION
	The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Channel(s):** Shows the device types and/or protocols that were specified for the report. • **File Name:** Shows the files that were specified for the report. The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) users having both allowed and denied access by the number of copied files. Table 2 lists the top N (where N is a specific number) users having both allowed and denied access by the amount of copied data. Table 3 lists the top N (where N is a specific number) users having allowed access by the number of copied files. Table 4 lists the top N (where N is a specific number) users having allowed access by the amount of copied data. Table 5 lists the top N (where N is a specific number) users having denied access by the number of copied files. Table 6 lists the top N (where N is a specific number) users having denied access by the amount of copied data. Tables 1, 3 and 5 have the following columns: • **User Name** Shows a user name. • **Access Count** Shows the number of access requests. Values in this column are sorted in descending order. Tables 2, 4 and 6 have the following columns: • **User Name** Shows a user name. • **Data Size** Shows the total size of all copied files. Values in this column are sorted in descending order.
Top copied files	This report shows the most frequently copied files, including e-mail attachments, sorted according to the number of copied files and total size of all copied files. By default, the report lists the first 10 files but you can specify any number of files. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed.

REPORT TYPE	DESCRIPTION
	The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running. • **Computer(s):** Shows the computers that were specified for the report. • **Users(s):** Shows the users that were specified for the report. • **Channel(s):** Shows the device types and/or protocols that were specified for the report. The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) copied files having both allowed and denied access by quantity. Tables 2 lists the top N (where N is a specific number) copied files having both allowed and denied access by size. Table 3 lists the top N (where N is a specific number) copied files having allowed access by quantity. Tables 4 lists the top N (where N is a specific number) copied files having allowed access by size. Table 5 lists the top N (where N is a specific number) copied files having denied access by quantity. Tables 6 lists the top N (where N is a specific number) copied files having denied access by size. Tables 1, 3 and 5 have the following columns: • **File Name** Shows a file name. • **Number of Files** Shows the number of copied files. Values in this column are sorted in descending order. Tables 2, 4 and 6 have the following columns: • **File Name** Shows a file name. • **Data Size** Shows the total size of all copied files. Values in this column are sorted in descending order.
Top active processes	This report shows the most active processes (applications) sorted according to the number of copied files and total size of all copied files. By default, the report lists the first 10 processes but you can specify any number of processes. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Channel(s):** Shows the device types and/or protocols that were specified for the report. • **File Name:** Shows the files that were specified for the report.

REPORT TYPE	DESCRIPTION
	The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) processes having both allowed and denied access by the number of copied files. Table 2 lists the top N (where N is a specific number) processes having both allowed and denied access by the amount of copied data. Table 3 lists the top N (where N is a specific number) processes having allowed access by the number of copied files. Table 4 lists the top N (where N is a specific number) processes having allowed access by the amount of copied data. Table 5 lists the top N (where N is a specific number) processes having denied access by the number of copied files. Table 6 lists the top N (where N is a specific number) processes having denied access by the amount of copied data. Tables 1, 3 and 5 have the following columns: • **Process Name** Shows a process name. • **Access Count** Shows the number of access requests. Values in this column are sorted in descending order. Tables 2, 4 and 6 have the following columns: • **Process Name** Shows a process name. • **Data Size** Shows the total size of all copied files. Values in this column are sorted in descending order.
Top copied files by extension	This report shows the most frequently copied file extensions sorted according to the number of copied files including e-mail attachments and total size of all copied files. By default, the report lists the first 10 file extensions but you can specify any number of file extensions. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Users(s):** Shows the users that were specified for the report. • **Channel(s):** Shows the device types and/or protocols that were specified for the report. The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) copied file extensions having both allowed and denied access by quantity. Tables 2 lists the top N (where N is a specific number) copied file extensions having both allowed and denied access by size. Table 3 lists the top N (where N is a specific number) copied file extensions having allowed access by quantity. Tables 4 lists the top N (where N is a specific number) copied file extensions having allowed access by size. Table 5 lists the top N (where N is a specific number) copied file extensions having denied access by

REPORT TYPE	DESCRIPTION
	quantity. Tables 6 lists the top N (where N is a specific number) copied file extensions having denied access by size. Tables 1, 3 and 5 have the following columns: • **Extension** Shows a file extension. • **Number of Files** Shows the number of copied files. Values in this column are sorted in descending order. Tables 1, 3 and 5 also have a **Total** row that sums up all the values in the **Number of Files** column. Tables 2, 4 and 6 have the following columns: • **Extension** Shows a file extension. • **Data Size** Shows the total size of all copied files. Values in this column are sorted in descending order. Tables 2, 4 and 6 also have a **Total** row that sums up all the values in the **Data Size** column. Each table is followed by a pie chart which represents the report results in percentages. The **No extension** label is used for all files without an extension, and the **Other** label is used for all file extensions whose combined percentage out of the total number of files is less than 5%. The **Direct access** label is used for all CD/DVD/BD burn and direct-write operations (e.g. formatting).
Top printed documents	This report shows the most frequently printed documents (files) sorted according to the number of printed files and total size of all printed files. By default, the report lists the first 10 documents but you can specify any number of documents. The report consists of three sections: the Report Header, Report Parameters, and Report Results. The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type. The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes: • **Period from: to:** Shows the start and end date and time of the report period for which data is displayed. *The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.* • **Computer(s):** Shows the computers that were specified for the report. • **Users(s):** Shows the users that were specified for the report. • **Printer(s):** Shows the printers that were specified for the report. The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) documents having both allowed and denied access by the number of printed files. Table 2 lists the top N (where N is a specific number) documents having both allowed and denied access by the amount of printed data. Table 3 lists the top N (where N is a specific number) documents having allowed access by the number of printed files. Table 4 lists the top N (where N is a specific number) documents having allowed access by the

REPORT TYPE	DESCRIPTION
	amount of printed data. Table 5 lists the top N (where N is a specific number) documents having denied access by the number of printed files. Table 6 lists the top N (where N is a specific number) documents having denied access by the amount of printed data. Tables 1, 3 and 5 have the following columns: • **File Name** Shows a document name. • **Number of Files** Shows the number of printed documents. Values in this column are sorted in descending order. Tables 2, 4 and 6 have the following columns: • **File Name** Shows a document name. • **Data Size** Shows the total size of all printed documents. Values in this column are sorted in descending order.

Configuring E-mail Delivery of Reports

DeviceLock allows you to distribute reports through e-mail. E-mail delivery of reports requires a Simple Mail Transfer Protocol (SMTP) server. Before you can use e-mail delivery of reports, you must specify which SMTP server will be used to send the e-mail messages and which e-mail address will be used as the sender address.

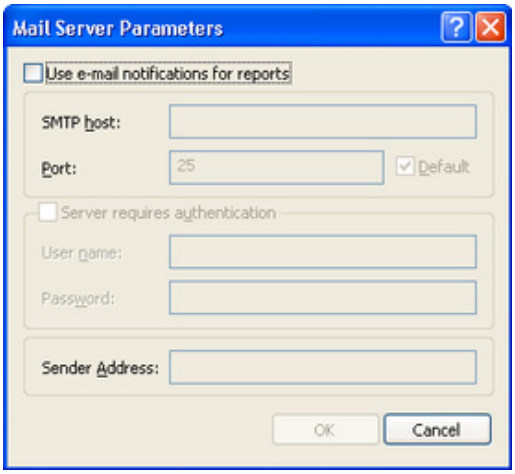
To configure e-mail delivery of reports

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, right-click **Reports**, and then click **Notification Settings**.

   – OR -

   Select **Reports**, and then click **Notification Settings** on the toolbar.

   The Mail Server Parameter dialog box appears.



4. In the **Mail Server Parameter** dialog box, do the following:

USE THIS	TO DO THIS
Use e-mail notifications for reports	Configure an e-mail notification for completed reports. Select the **Use e-mail notifications for reports** check box to type your e-mail information in the corresponding boxes. Clear the **Use e-mail notifications for reports** check box to remove the previously configured SMTP server and e-mail notification settings.
SMTP host	Specify the name of the SMTP server to use when sending messages. You can specify the SMTP server through an IP address or a DNS resolvable name.
Port	Specify the port that SMTP clients use to connect to the SMTP server. The default value is 25. **Note:** Both non-SSL (unencrypted) and SSL connections to the specified SMTP server are supported. DeviceLock automatically identifies encrypted connections and their type.
Server requires authentication	Specify the type of authentication to use with the SMTP server. Select the **Server requires authentication** check box to specify basic authentication. Clear the **Server requires authentication** check box to specify no authentication.
User name	Specify the user name to use for authentication with the SMTP server. This property requires a value if you specified basic authentication.
Password	Specify the password to use for authentication with the SMTP server. This property requires a value if you specified basic authentication.
Sender Address	Specify the e-mail address that will be used in the **From:** line of an e-mail message.

5. Click **OK**.

Setting Default Format for Reports

You can specify the report output format you want to use for reports. The available options are:

- HTML Format (*.htm)
- PDF Format (*.pdf)

- Rich Text Format (*.rtf)

DeviceLock uses PDF as the default output format for reports.

To set the default format for reports

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, right-click **Reports**. Next point to **Set Default Format**, and then click any of the following options: **HTML**, **PDF**, **RTF**.

Defining Report Parameters

Report parameters help you specify which data from the DeviceLock log files you want to use in a report. For example, you can specify a date range to restrict the data that appears in the report. Report parameters must be set for each report individually.

To define report parameters, use the **Report Options** dialog box. This dialog box appears in one of the following situations:

- When you right-click any report template in the console tree, and then click **New Report**.
- When you select any report template in the console tree, and then click **New report** on the toolbar.

Report Options Dialog Box

Period from:……**To:**
Specifies the start and end date and time of the report period for which data is displayed. The date format is *MM/DD/YYYY* where *MM* specifies the month, *DD* the day, *YYYY* the year. The time format is *hh:mm:ss {AP}M*, where *hh* the hour, *mm* the minute, *ss* the second, and *{AP}M* the AM or PM designation.

In the **Period from:** and **To:** boxes, type or select the date and time of the report period.

The default start and end time of the report period is the time at which the **Report Options** dialog box opens. The default end date of the report period is the current date. The default start date of the report period is the same day in an earlier month. For example, if the current date is March 5, 2009, the default end date of the report period is 3/5/2009 while the default start date is 2/5/2009.

Computer(s):
Specifies computers for the report. The **Computer(s)** box is not displayed in the **Report Options** dialog box for the Top active computers report types.

The **Computer(s)** box is empty by default. This means that the report will display data for all computers in the DeviceLock Enterprise Server database.

To specify computers for the report, you can do any of the following:

- In the **Computer(s)** box, type computer names using wildcards, such as asterisks (*) and question marks (?). For example, if you specify ***.mydomain.com**, the report will display data for all computers in mydomain.com.

  An asterisk (*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity.

  Multiple computer names must be separated by a comma (,) or semicolon (;).

  - OR -

- Click **Browse** next to the **Computer(s):** box, and then do the following:

  a) When the **Edit computers list** dialog box opens to the **Select computer(s)** list, click one of the following options:

OPTION	DESCRIPTION
Active Directory	This option is selected by default. This option lets you select computers from the Active Directory tree. If you select this option: 1. Click the ellipsis button [...] to open the **Credentials** dialog box and supply alternative credentials to access Active Directory. For more information, see the description of Active Directory credentials. 2. In the left pane of the **Edit computers** dialog box, select the appropriate check boxes next to desired computers. 3. Click the right single-arrow button [>]. *The selected computers are displayed under Selected computers in the right pane of the dialog box.* *To remove single computers from the list of selected computers, use the left single-arrow button [<].* *To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button [>>] or left double-arrow button [<<].*
From Database	This option lets you select computers from the DeviceLock Enterprise Server database that shows all computers from which the server has ever received audit and shadow data. If you select this option: 1. In the left pane of the **Edit computers** dialog box, select the appropriate check boxes next to desired computers. 2. Click the right single-arrow button [>]. *The selected computers are displayed under Selected computers in the right pane of the dialog box.* *To remove single computers from the list of selected computers, use the left single-arrow button [<].* *To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button [>>] or left double-arrow button [<<].*

OPTION	DESCRIPTION
LDAP	This option lets you select computers from the LDAP (Lightweight Directory Access Protocol) tree. If you select this option: 1. Click the ellipsis button [...] to open the **LDAP Settings** dialog box and configure a connection to the LDAP server. For more information, see the description of LDAP settings. 2. In the left pane of the **Edit computers** dialog box, select the appropriate check boxes next to desired computers. 3. Click the right single-arrow button [>]. *The selected computers are displayed under Selected computers in the right pane of the dialog box.* *To remove single computers from the list of selected computers, use the left single-arrow button* [<]. *To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button* [>>] *or left double-arrow button* [<<].
From File	This option lets you select computers from an external text file. A text file must contain each computer's name or IP address on a separate line and can be either Unicode or non-Unicode. If you select this option: 1. Click the ellipsis button [...] to open the **Open** dialog box and browse for the file to use. 2. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import. 3. In the folder list, locate and open the folder that contains the file. 4. Click the file, and then click **Open**. *The computers from the file are displayed in the left pane of the Edit computers list dialog box.* 5. In the left pane of the **Edit computers** dialog box, select the desired computers, and then click the right single-arrow button [>]. *The selected computers are displayed under Selected computers in the right pane of the dialog box.* *To remove single computers from the list of selected computers, use the left single-arrow button* [<]. *To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button* [>>] *or left double-arrow button* [<<].
Manual	This option lets you manually add computers that you want to select for the report. If you select this option: 1. In the left pane of the **Edit computers list** dialog box, type either computer names or IP addresses. Press the ENTER key after each computer name to make sure that each computer name is on a separate line. 2. In the left pane of the **Edit computers** dialog box, select the desired computers, and then click the right single-arrow button [>]. *The selected computers are displayed under Selected computers in the right pane of the dialog box.*

OPTION	DESCRIPTION
	To remove single computers from the list of selected computers, use the left single-arrow button . *To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button* *or left double-arrow button* .

b) Click **OK**.

Version(s):
Specifies DeviceLock Service versions for the report. Appears only for the DeviceLock Service versions and DeviceLock Service versions by computers report types. The **Version(s)** box is empty by default. This means that the report will display data for computers with all versions of DeviceLock Service in the DeviceLock Enterprise Server database.

To specify versions for the report, in the **Version(s)** box, type version numbers using wildcards, such as asterisks (*) and question marks (?). For example, type **6.4.?** to specify version 6.4.x.

An asterisk (*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity.

Multiple versions must be separated by a comma (,) or semicolon (;).

Users
Specifies users for the report. The **User(s)** box is not displayed in the **Report Options** dialog box for the Top active computers, Top active users, and Top active processes report types.

The **User(s)** box is empty by default. This means that the report will display data for all users in the DeviceLock Enterprise Server database.

To specify users for the report, do one of the following:

- In the **User(s) box**, specify user names using wildcards, such as asterisks (*) and question marks (?). For example, if you specify **mydomain***, the report will display data for all users in mydomain.com.
  An asterisk (*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity.
  Multiple user names must be separated by a comma (,) or semicolon (;).

  Note: You cannot specify user groups for the report.

  - OR -

- Click **Browse** next to the **User(s)** box, and then do the following:
  a) In the **Select Users** dialog box that opens, in the **Enter the object names to select** box, type the user account names that you want to specify for the report.
  Multiple user names must be separated by a semicolon (;).
  b) Click **OK**.

File name
Specifies files for the report. Appears only for the Top active users, Top active computers, Top active processes, and Copied files per channel report types in the Shadow Log report category.

The **File name** box is empty by default. This means that the report will display data for all files in the DeviceLock Enterprise Server database.

To specify files for the report, in the **File name** box, type file names using wildcards, such as asterisks (*) and question marks (?). For example, type ***.txt** to specify all files that have the .txt extension. To continue the example, if you want to specify all files whose names begin with any characters that contain the string "price" and have any extension, type ***price*.***

An asterisk (*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity.

Multiple file names must be separated by a comma (,) or semicolon (;).

Printer(s):
Specifies printer names for the report. Appears only for the Top printed documents report type. The **Printer(s)** box is empty by default. This means that the report will display data for all printers available in the DeviceLock Enterprise Server database.

To specify printer names for the report, in the **Printer(s)** box, type names using wildcards, such as asterisks (*) and question marks (?). For example, type **PDF*** to specify all printers whose names begin with PDF.

An asterisk (*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity.

Multiple names must be separated by a comma (,) or semicolon (;).

Threshold
Specifies the time interval, in seconds, between logged events. This interval is used for event consolidation. It appears for all report types in the Audit Log report category except the Top inserted USB & FireWire devices report type.

Because a single user action often triggers multiple events, DeviceLock uses event consolidation when collecting events from the audit log for reporting purposes. DeviceLock compares the time element of an event with the time of subsequent events. When this time delta is less than or equal to the **Threshold** value, multiple events of the same type (either Allowed or Denied) are combined into a single summary event if all of the following conditions are true:

- The events are associated with the same computer;
- The events are associated with the same device type.

Report Devices
Select this option if you want to display data for all device types. If you do not select this option, information on all device-related activities will be excluded from the report. Appears only for Allowed & Denied access requests per channel, Allowed vs. Denied access requests, and Copied files per channel report types.

Report TS Devices as regular devices
Select this option if you want to count TS Devices data together with regular devices data:

- TS Devices (Mapped drives) -> Removable
- TS Devices (Serial port) -> Serial port
- TS Devices (USB devices) -> USB Devices
- TS Devices (Clipboard) -> Clipboard

If you do not select this option, data related to TS Devices will be counted and displayed separately. Appears only for Allowed & Denied access requests per channel, Read & Write access requests per device type, and Copied files per channel report types.

Report Protocols
Select this option if you want to display data for all protocols. If you do not select this option, information on all protocol-related activities will be excluded from the report. Appears only for Allowed & Denied access requests per channel, Allowed vs. Denied access requests, and Copied files per channel report types.

Send report via email
Select this option if you want to automatically send the generated report to individual users through e-mail. If you select this option, in the **Recipients** box, type the e-mail addresses of the recipients separated by commas, semicolons, or spaces.

Use the following format: *user*@*mailserver*.

Access type(s)
Specifies the types of events that you want to include in or exclude from the report. Appears only for the Read & Write access requests per device type report type in the Audit Log report category.

If you select the **Allowed** check box, the Success Audit events (that is, events that record successful access attempts) will be retrieved for the report. If you select the **Denied** check box, the Failure Audit events (that is, events that record failed access attempts) will be retrieved for the report. You can use either or both of these options to specify the types of events.

Device type(s)
Specifies the device types for the report. Appears only for the Top active computers, Top active users, Top copied files, Top active processes, and Top copied files by extension report types.

If you select this option, select the appropriate check boxes next to the device types you want to specify for the report.

Protocol(s)
Specifies the protocols for the report. Appears only for the Top active computers, Top active users, Top copied files, Top active processes, and Top copied files by extension report types.

If you select this option, select the appropriate check boxes next to the protocols you want to specify for the report.

Note: If you leave both options - **Device type(s)** and **Protocol(s)** unselected, the report will display data for all device types and protocols. If you select either of these options and then specify device type(s) or protocols, the report will display data only for the specified device type(s) or protocols.

You may also select the Other protocol, which represent data transmitted via unrecognized protocols logged by Protocols White List (Any and SSL) and Basic IP Firewall rules.

Top computers
Specifies the number of the most frequently used computers. Appears only for the Top active computers report type.

The default value is 10. To change the default value, type or select the appropriate number of computers in the **Top computers** box.

Top Printers
Specifies the number of the most frequently used printers. Appears only for the Top used Printers report type.

The default value is 10. To change the default value, type or select the appropriate number of printers in the **Top Printers** box.

Top users
Specifies the number of the most active users. Appears only for the Top active users report type.

The default value is 10. To change the default value, type or select the appropriate number of users in the **Top users** box.

Top USB and FireWire devices
Specifies the number of the most frequently inserted USB and FireWire devices. Appears only for the Top inserted USB & FireWire devices report type.

The default value is 10. To change the default value, type or select the appropriate number of devices in the **Top USB and FireWire devices** box.

Top USB devices
Specifies the number of the most frequently used USB devices. Appears only for the Top used USB devices report type.

The default value is 10. To change the default value, type or select the appropriate number of devices in the **Top USB devices** box.

Top processes
Specifies the number of the most active processes. Appears only for the Top active processes report type.

The default value is 10. To change the default value, type or select the appropriate number of processes in the **Top processes** box.

Top files
Specifies the number of the most frequently copied files. Appears only for the Top copied files and Top copied files by extension report types.

The default value is 10. To change the default value, type or select the appropriate number of files in the **Top files** box.

Top printed documents
Specifies the number of the most frequently printed documents. Appears only for the Top printed documents report type.

The default value is 10. To change the default value, type or select the appropriate number of documents in the **Top printed documents** box.

Managing Reports

Managing DeviceLock reports involves the following tasks:

- Running reports
- Refreshing reports
- Viewing reports
- Viewing report parameters
- Exporting and saving reports
- Sending reports through e-mail
- Deleting reports

Running Reports

To run a report

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Reports**.
4. Expand **Audit Log** or **Shadow Log**.
5. Under **Audit Log** or **Shadow Log**, right-click any report template you want to use, and then click **New report**.

   The Report Options dialog box appears.
6. In the **Report Options** dialog box, accept or change the default settings, and then click **OK**.

   For information on the default settings and changing the default settings in the Report Options dialog box, see "Defining Report Parameters."

   While the report is being processed on DeviceLock Enterprise Server, the report execution information is displayed in DeviceLock Management Console. To view and analyze this information, in the console tree select the report template that you used for running a new report.

   When you select a report template in the console tree, in the details pane you can view report execution information regarding all reports based on the selected template. Report execution information includes the following:

   - **User** – the name of the user who ran the report.
   - **From Computer** – the name of the computer used to run the report.

- **Started** – the date and time when the report began to run.
- **Finished** – the date and time when the report was finished.
- **E-mailed** – possible values: **Yes** and **No**. **Yes** indicates that the report included in the e-mail delivery was successfully delivered to some or all of the intended recipients. **Yes** is displayed only after the sending process is complete. **No** indicates one of the following:

  The report is not included in the e-mail delivery.

  - OR -

  The report included in the e-mail delivery did not reach all of the intended recipients.

  If an error occurs during the e-mail delivery of a report, you can use Server Log Viewer to determine the reason. For more information on Server Log Viewer, see "Server Log Viewer."

  If your computer has anti-virus or anti-spam software installed and running and an error occurs during the e-mail delivery of a report, the error information may not be reported in the DeviceLock Enterprise Server log. This behavior occurs because anti-virus and anti-spam products, for example, Symantec Norton AntiVirus, can automatically intercept e-mail traffic.

  For information about how your anti-virus or anti-spam program works, consult the manufacturer's documentation included with your program.

- **Status** – possible values: **Generating**, **Ready**, **Error**. **Generating** indicates that the report is being generated. **Ready** indicates that the report was successfully completed. **Error** indicates that an error occurred while the report was being generated.

  If an error occurs while the report is being generated, you can do the following to determine the reason:

  Click the error report to display the error message.

  - OR -

  Use Server Log Viewer. For more information on Server Log Viewer, see "Server Log Viewer."

Refreshing Reports

Because current reports and the current status of reports are not updated automatically, you need to perform a refresh operation.

To refresh reports

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Reports**.
4. Expand **Audit Log** or **Shadow Log**.
5. Under **Audit Log** or **Shadow Log**, right-click any report template, and then click **Refresh**.

   - OR -

   Under **Audit Log** or **Shadow Log**, select the report template that you used for generating reports, and then do one of the following:

- Click **Refresh** on the toolbar.
  - OR -
- In the details pane, right-click any report, and then click **Refresh**.

When you select a report template in the console tree, you can view the reports associated with it in the details pane.

Viewing Reports

After a report is successfully completed, you can open it in DeviceLock Management Console.

To view a report

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Reports**.
4. Expand **Audit Log** or **Shadow Log**.
5. Under **Audit Log** or **Shadow Log**, select the report template that you used for generating the report you want to view.

   When you select a report template in the console tree, you can view the reports associated with it in the details pane.

6. In the details pane, right-click the report you want to view, and then click **Open**.

   The report opens in the application associated with the report default format you chose. By default, the report opens in the Adobe Acrobat Reader, because DeviceLock uses PDF as the default output format for reports.

   If you want to open a report in PDF format, you must have Adobe Acrobat Reader installed on your computer. You can download Acrobat Reader from the Adobe Web site: http://get.adobe.com/reader/.

Viewing Report Parameters

After you run a report, you can get information on the report parameters that you specified when generating the report.

To view report parameters

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Reports**.
4. Expand **Audit Log** or **Shadow Log**.
5. Under **Audit Log** or **Shadow Log**, select the report template that you used for generating the report.

When you select a report template in the console tree, you can view the reports associated with it in the details pane.

6. In the details pane, right-click the report, and then click **View parameters**.

   The Report Options dialog box appears. In this dialog box, you can view the parameter values that you specified when generating the report.

Exporting and Saving Reports

DeviceLock provides the ability to export generated reports to another format (such as HTML, PDF or RTF) and save them as files locally or on your network.

Note: When you save a report as HTML, it is saved as an .htm file. If this report contains graphic images, each image is saved as a .gif file in the same directory as the .htm file.

To export and save reports

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Reports**.
4. Expand **Audit Log** or **Shadow Log**.
5. Under **Audit Log** or **Shadow Log**, select the report template that you used for generating the report you want to export and save.

   When you select a report template in the console tree, you can view the reports associated with it in the details pane.

6. If you want to export and save a single report, do the following:
   a) In the details pane, right-click the report you want to export and save, point to **Save As**, and then click any of the following options: **HTML**, **PDF**, **RTF**.
   The Save As dialog box appears.
   b) In the **Save As** dialog box, in the **Save** in box, browse to the location where you want to save the report.
   c) In the **File** name box, type the file name you want.
   By default, the file name is {Report_Type}- [{dd.mm.yy hh:mm:ss}] where {dd.mm.yy hh:mm:ss} is the current date and time.
   d) Click **Save**.

   If you save a report as HTML and the report contains one or more graphic images, the images will be extracted from the report and saved as separate .gif files along with the .htm file in the same directory.
7. If you want to export and save multiple reports, do the following:
   a) In the details pane, select multiple reports by holding down the SHIFT key or the CTRL key while clicking them.
   b) Right-click the selection, point to **Save As**, and then click any of the following options: **HTML**, **PDF**, **RTF**.
   The Browse for folder dialog box appears.

c) In the **Browse for folder** dialog box, select the folder in which you want to save the reports, and then click **OK**.

Sending Reports Through E-mail

DeviceLock provides the ability to send generated reports through e-mail.

To send generated reports through e-mail

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Reports**.
4. Expand **Audit Log** or **Shadow Log**.
5. Under **Audit Log** or **Shadow Log**, select the report template that you used for generating the report you want to send through e-mail.

   When you select a report template in the console tree, you can view the reports associated with it in the details pane.

6. In the details pane, right-click the report you want to send, and then click **Send via e-mail**.

   You can select multiple reports by holding down the SHIFT key or the CTRL key while clicking them.

   The Send report via e-mail dialog box appears.

7. In the **Send report via e-mail** dialog box, in the **Recipients** box, type the e-mail addresses of the recipients separated by commas, semicolons, or spaces. Use the following format: *user@mailserver.*
8. Click **OK**.

   If an error occurs during the e-mail delivery of a report, an appropriate error message will be logged. You can use Server Log Viewer to determine the reason. For more information on Server Log Viewer, see "Server Log Viewer."

Note: When you send a report in HTML format, the report is included in the body of the e-mail message and is not sent as an attachment.

Deleting reports

You can delete reports when they are no longer required.

To delete reports

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Reports**.
4. Expand **Audit Log** or **Shadow Log**.

5. Under **Audit Log** or **Shadow Log**, select the report template that you used for generating the report you want to delete.

   By selecting a report template in the console tree, you can view the reports associated with it in the details pane.

6. In the details pane, right-click the report you want to delete, and then click **Delete**.

   You can delete multiple reports at the same time. To do this, do the following:

   a) In the details pane, select multiple reports by holding down the SHIFT key or the CTRL key while clicking them.
   b) Right-click the selection, and then click **Delete**.

DeviceLock Security Policies (Offline Profile)

Today, organizations have many users who must continue working with business-critical information when they are disconnected from the corporate network. For example, traveling sales representatives, insurance agents and regional inspectors increasingly use corporate laptops or notebooks at disconnected locations. Protecting the sensitive information on these mobile computers has become a priority for many organizations.

DeviceLock provides greater protection of sensitive corporate information in disconnected environments. Now you can control user access to devices and protocols as well as shadow copying of the data written by the user or transmitted over the network in different offline scenarios. DeviceLock also offers more management flexibility, as you can define different online vs. offline security policies for the same user or set of users.

A user's online policies are applied when connected to the corporate network, or specified DeviceLock Enterprise Servers, or Active Directory domain controllers. Offline policies are applied when the user is working disconnected from the corporate network, or specified DeviceLock Enterprise Servers, or Active Directory domain controllers.

To configure DeviceLock to enforce different policies for online vs. offline scenarios begin by setting permissions for two profile types:

- **Regular Profile**. These settings are used by client computers that are working online.
- **Offline Profile**. These settings are used by client computers that are working offline, for example, when corporate users travel with laptop computers. If offline profile settings are not configured, regular profile settings are used instead.

You can use different regular vs. offline profiles for Permissions, Auditing, Shadowing rules and Alerts, USB Devices White List, Media White List, Protocols White List, Content-Aware Rules, Basic IP Firewall, and Security Settings. You can manage offline profile settings using DeviceLock Management Console, DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.

The following examples describe typical scenarios in which you are likely to set different online vs. offline security policies to better protect your corporate data.

- **Scenario 1.** Suppose you have a Finance group in your organization. As an administrator, you can allow members of this group to write files to Removable, Optical Drive, USB, and Floppy devices when they work online. Their online activity will be audited. Any copied files will be shadow copied; and audit and shadow logs will be sent to DeviceLock Enterprise Server. When offline, members of the Finance group will be denied write access.
  These security policies let you monitor the activity of the Finance group members in real-time mode. By examining audit and shadow logs on DeviceLock Enterprise Server (often on a daily basis), you can respond promptly and appropriately when a

data leakage incident occurs. In this case, a user will not be able to copy sensitive information to a device while offline in an attempt to avoid sending shadow copies to DeviceLock Enterprise Server and thus alerting the Security department of the data theft.

- **Scenario 2.** Imagine Mary, a sales representative of a large company, who has a notebook computer and frequently works out of the office. She needs to be able to provide her business partners with information files resulting from her work. In this situation, you can allow Mary to write certain files to Removable, Optical Drive, USB, and Floppy devices and enable shadow copying of these files when she works offline. When online, she will be denied write access to the specified device types.
  These security policies give you greater flexibility in managing users within an organization while providing better corporate data security.

Configuring Offline Mode Detection Settings

You can define the network characteristics that DeviceLock uses to detect its connection state (whether it is online or offline). By default, DeviceLock works in offline mode when the network cable is not connected to the client computer.

To configure offline mode detection settings

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

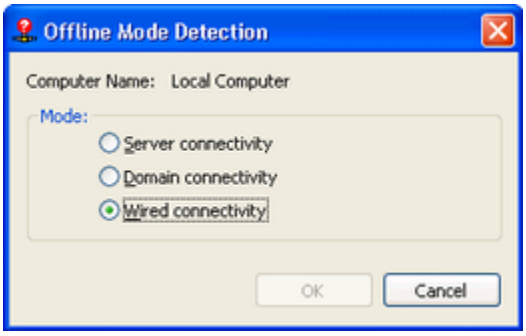
   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Select **Service Options**.

   When you select Service Options in the console tree, they are displayed in the details pane.

3. In the details pane, do one of the following:
   - Right-click **Offline mode detection**, and then click **Properties**.
     - OR -
   - Double-click **Offline mode detection**.

   The Offline Mode Detection dialog box appears.



4. In the **Offline Mode Detection** dialog box, click any of the following options:

OPTION	DESCRIPTION
Server connectivity	Indicates that the connection state of a client computer is determined by whether or not it can connect to the specified DeviceLock Enterprise Server. Thus, a client computer works in online mode, if it can connect to any of the specified DeviceLock Enterprise Servers and send them audit and shadow logs. A client computer works in offline mode if it cannot authenticate with any of the specified DeviceLock Enterprise Servers or all of the specified DeviceLock Enterprise Servers become unavailable at the same time. **Best Practice:** The most reliable way to secure client/server communication is to use DeviceLock Certificate authentication. For client/server certificate authentication, the public key must be installed on client computers, while the private key must be installed on DeviceLock Enterprise Server(s). If the certificate (the public key) is installed only on client computers, the server will reject connections and client computers will work in offline mode. If the certificate (the private key) is installed only on DeviceLock Enterprise Server, the server and the client will authenticate each other once a connection is established though this type of authentication is less secure than certificate-based authentication. For detailed information on DeviceLock Certificates, see "DeviceLock Certificates."
Domain connectivity	Indicates that the connection state of a client computer is determined by whether or not it can connect to the appropriate Active Directory domain controller (a domain controller of the domain to which the client computer belongs). Thus, a client computer works in online mode, if it can connect to the appropriate domain controller. A client computer works in offline mode, if the appropriate domain controller becomes unavailable. *A client computer that is not joined to a domain (a workgroup or stand-alone computer) always works in offline mode.*

OPTION	DESCRIPTION
Wired connectivity	Indicates that the connection state of a client computer is determined by whether or not the network cable is connected to the Network Interface Card (NIC). This is the simplest and least secure method of detecting the connection state. Thus, a client computer works in online mode, if the network cable is connected to the NIC. A client computer works in offline mode, if the network cable is disconnected from the NIC. Please note that wireless network connections (WiFi, etc.) and modem connections are ignored. This option is selected by default.

5. Click **OK**.

Switching Between Online and Offline Mode

DeviceLock Service running on client computers automatically detects the connection state and seamlessly switches between online and offline mode every hour and when any of the following events occurs:

- A user boots the computer running DeviceLock Service.
  DeviceLock Service always starts in offline mode.
- A user logs on.
- A user right-clicks the DeviceLock Tray Notification Utility icon in the notification area of the taskbar, and then clicks **Refresh Current State**.
  The DeviceLock Tray Notification Utility icon is displayed in the notification area when Always show tray icon is enabled in Service Options.
- DeviceLock Service sends audit and shadow logs to DeviceLock Enterprise Server.
- A network interface changes state:
  a) A network cable is connected or disconnected.
  b) A modem connects or disconnects.
  c) A virtual private network (VPN) connection is established or terminated.
  d) A wireless network connection using a WiFi card is established or terminated.
  e) A DHCP-assigned IP address is used or released.
  f) A network card is enabled, disabled, added or removed.
- Changes to DeviceLock Service settings are made.

Managing Offline Security Policies for Devices

You can manage offline security policies in much the same way as you manage online (regular) policies except for a few variations. This section provides offline profile-specific information as well as basic management procedures. For detailed information on

Permissions, audit, shadowing rules and alerts, white lists, Content-Aware Rules, and Security Settings for devices, refer to the following sections of the User Manual: "Permissions (Regular Profile)", "Auditing, Shadowing & Alerts (Regular Profile)", "USB Devices White List (Regular Profile)", "Media White List (Regular Profile)", "Security Settings (Regular Profile)", "Content-Aware Rules for Devices (Regular Profile)."

Managing offline security policies for devices involves the following operations:

- Managing offline Permissions
- Managing offline audit, shadowing rules and alerts
- Managing the offline USB Devices White List
- Managing the offline Media White List
- Managing offline Content-Aware Rules
- Managing offline Security Settings

You can manage offline security policies by using DeviceLock Management Console, Service Settings Editor, or DeviceLock Group Policy Manager.

Managing Offline Permissions

For a detailed description of the Permissions feature, see "Permissions (Regular Profile)."

Offline permissions can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that permissions on a device type are not set. This is the default state.
Configured	Indicates that permissions on a device type are set.
Full Access	Indicates that full access rights are granted to the Everyone account.
No Access	Indicates one of the following: • The Everyone account has No Access permissions and is the only account assigned to a device type. *No Access permissions assigned to the Everyone account take priority over permissions assigned to other accounts.* • All users and groups assigned to a device type have No Access permissions. • All users and groups assigned to a device type are removed.

STATE	DESCRIPTION
Use Regular	Indicates that the inheritance of offline permissions is blocked and regular permissions are enforced. Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of regular permissions is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of regular permissions lets you prevent offline permissions inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of regular permissions, see "Removing Offline Permissions."

Managing offline permissions involves the following tasks:

- Setting and editing offline permissions
- Undefining offline permissions
- Removing offline permissions

Setting and Editing Offline Permissions

To set and edit offline permissions

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

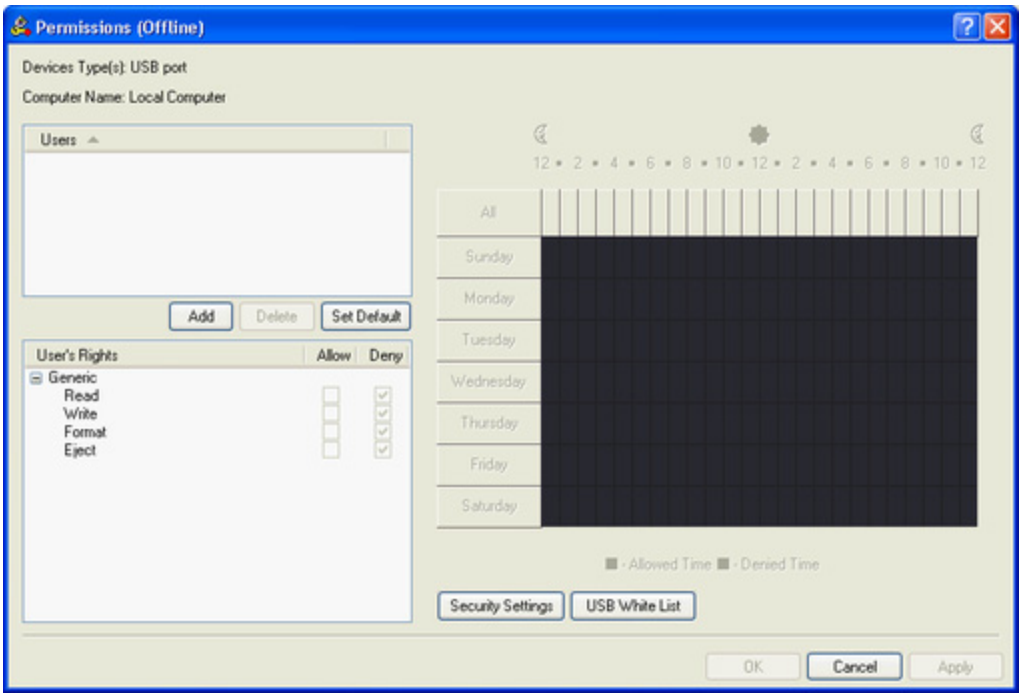
   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Permissions**.

   When you select Permissions in the console tree, in the details pane you can view device types for which you can set permissions. In the details pane, you can also view the current state of offline permissions for each device type in the Offline column.

4. In the details pane, do one of the following:
   - Right-click the device type for which you want to set or edit permissions, and then click **Set Offline Permissions**.
     - OR -

- Select the device type for which you want to set or edit permissions, and then click **Set Offline Permissions** on the toolbar.

The Permissions (Offline) dialog box appears.



5. In the **Permissions (Offline)** dialog box, do the following:

TO DO THIS	FOLLOW THESE STEPS
To set the default permissions	• In the upper-left pane of the dialog box, under **Users**, click **Set Default**. *The default permissions are assigned to the Administrators, Everyone, and SYSTEM accounts. For information about which permissions are set for these accounts by default, see "Permissions (Regular Profile)."*
To set permissions for an additional user or group	1. In the upper-left pane of the dialog box, under **Users**, click **Add**. *The Select Users or Groups dialog box appears.* 2. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**. *The users and groups that you added are displayed under Users in the upper-left pane of the Permissions (Offline) dialog box*. 3. In the upper-left pane of the **Permissions (Offline)** dialog box, under **Users**, select the user or group. *You can select multiple users and/ or groups by holding down the SHIFT key or the CTRL key while clicking them*. 4. In the lower-left pane of the **Permissions (Offline)** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate access rights. *In the right pane of the Permissions (Offline) dialog box, you can set day and time restrictions that narrow user access to devices*.

TO DO THIS	FOLLOW THESE STEPS
	Use the left mouse button to select days and hours when the selected user or group will have access to devices. Use the right mouse button to mark days and hours when the selected user or group will not have access to devices.
To change permissions for an existing user or group	1. In the upper-left pane of the dialog box, under **Users**, select the user or group. 2. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate access rights.
To remove an existing user or group and permissions	• In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

6. Click **OK** or **Apply**.

Undefining Offline Permissions

You can reset previously set offline permissions to the unconfigured state. If offline permissions are undefined, regular permissions are applied to offline client computers.

To undefine offline permissions

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Permissions**.

   When you select Permissions in the console tree, in the details pane you can view device types for which you can set permissions. In the details pane you can also view the current state of offline permissions for each device type in the Offline column.

4. In the details pane, right-click the device type for which you want to undefine offline permissions, and then click **Undefine Offline**.

   You can undefine offline permissions set for several device types at the same time. To do this, do the following:

a) In the details pane, select several device types by holding down the SHIFT key or the CTRL key while clicking them.
b) Right-click the selection, and then click **Undefine Offline**.

The offline state of the permissions changes to "Not Configured."

Removing Offline Permissions

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of higher-level offline permissions and enforce regular permissions on specific lower-level groups of client computers. To enforce regular permissions, you must remove offline permissions.

To remove offline permissions

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Permissions**.

   When you select Permissions in the console tree, in the details pane you can view device types for which you can set permissions. In the details pane you can also view the current state of offline permissions for each device type in the Offline column.

4. In the details pane, right-click the device type for which you want to remove offline permissions, and then click **Remove Offline**.

   You can remove offline permissions set for several device types at the same time. To do this, do the following:
   a) In the details pane, select several device types by holding down the SHIFT key or the CTRL key while clicking them.
   b) Right-click the selection and then click **Remove Offline**.

   The offline state of the permissions changes to "Use Regular."

   The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline Audit, Shadowing and Alerts

For a detailed description of the Auditing & Shadowing feature, see "Auditing, Shadowing & Alerts (Regular Profile)." For a detailed description of the Alerts feature, see "Alerts." For information about how to enable online (regular) alerts, see "Auditing, Shadowing & Alerts (Regular Profile)." For information about how to enable offline alerts, see "Enabling Offline Alerts."

Offline audit, shadowing rules and alerts can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that audit, shadowing rules and alerts are not defined for a device type. This is the default state.
Configured	Indicates that audit, shadowing rules and alerts are defined for a device type.
No Audit	Indicates one of the following: • Audit rights are not set for all of the users and groups specified in audit and shadowing rules for a device type • All users and groups specified in audit and shadowing rules for a device type are removed. • The Everyone account has no Audit and Shadowing rights and is the only account specified in audit and shadowing rules for a device type.
Use Regular	Indicates that the inheritance of offline audit and shadowing rules is blocked and regular audit and shadowing rules are enforced. Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of regular rules is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of regular rules lets you prevent offline rules inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of regular rules, see "Removing Offline Audit and Shadowing Rules."

Managing offline audit, shadowing rules and alerts involves the following tasks:

- Defining and editing offline audit and shadowing rules
- Enabling offline alerts
- Undefining offline audit and shadowing rules
- Removing offline audit and shadowing rules

Defining and Editing Offline Audit and Shadowing Rules

To define and edit offline audit and shadowing rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

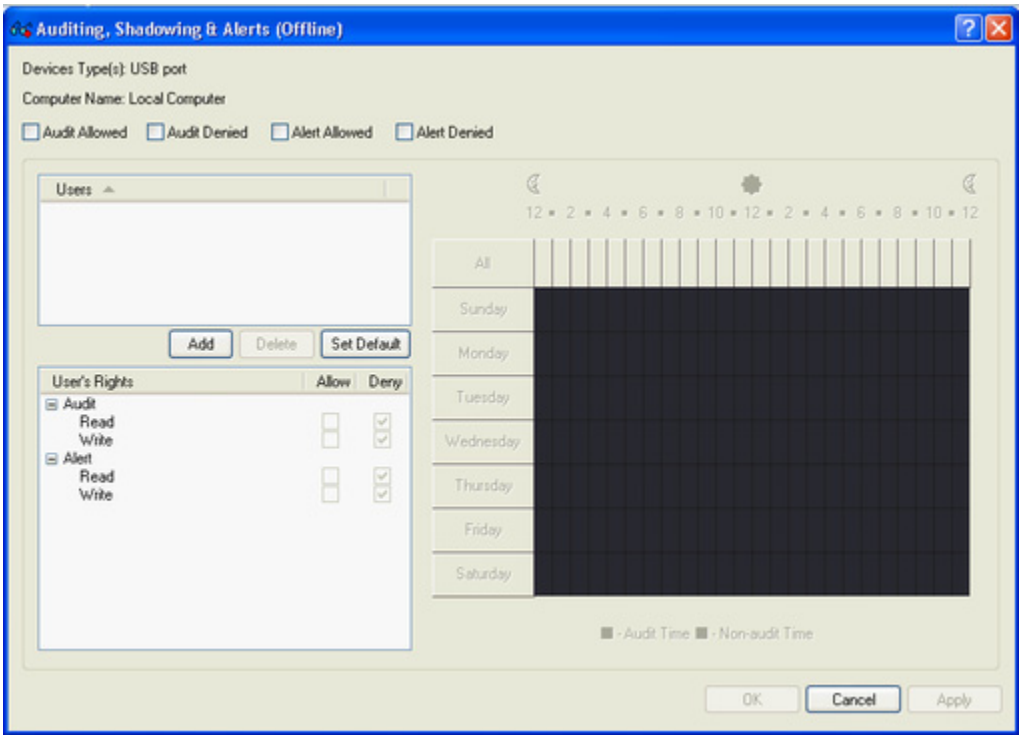
2. Expand **Devices**.
3. Under **Devices**, select **Auditing, Shadowing & Alerts**.

When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view device types for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each device type in the Offline column.

4. In the details pane, do one of the following:

- Right-click the device type for which you want to define or edit rules, and then click **Set Offline Auditing, Shadowing & Alerts**.
  - OR -
- Select the device type for which you want to define or edit rules, and then click **Set Offline Auditing, Shadowing & Alerts** on the toolbar.

The Auditing, Shadowing & Alerts (Offline) dialog box appears.



5. In the **Auditing, Shadowing & Alerts (Offline)** dialog box, do the following:

TO DO THIS	FOLLOW THESE STEPS
To define the default audit and	1. In the upper-left area of the dialog box, specify which events are written to the audit log. Select the **Audit Allowed** check box to audit successful attempts to gain access to a device. Select the **Audit Denied** check box to audit unsuccessful attempts to gain

TO DO THIS	FOLLOW THESE STEPS
shadowing rules	access to a device. 2. In the upper-left pane of the dialog box, under **Users**, click **Set Default**. *The default audit, shadowing rules and alerts apply to members of the Users group and Everyone account. For information about which Audit and Shadowing rights are set for these accounts by default, see "Auditing, Shadowing & Alerts (Regular Profile)."*
To define audit and shadowing rules for an additional user or group	1. In the upper-left area of the dialog box, specify which events are written to the audit log. Select the **Audit Allowed** check box to audit successful attempts to gain access to a device. Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a device. 2. In the upper-left pane of the dialog box, under **Users**, click **Add**. *The Select Users or Groups dialog box appears*. 3. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**. *The users and groups that you added are displayed under Users in the upper-left pane of the Auditing, Shadowing & Alerts (Offline) dialog box*. 4. In the upper-left pane of the **Auditing, Shadowing & Alerts (Offline)** dialog box, under **Users**, select the user or group. *You can select multiple users and/ or groups by holding down the SHIFT key or the CTRL key while clicking them*. 5. In the lower-left pane of the **Auditing, Shadowing & Alerts (Offline)** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate audit and shadowing rights. *Audit and Shadowing rights determine which user actions on devices are logged to the audit and/or shadow log*. *In the right pane of the Auditing, Shadowing & Alerts (Offline) dialog box, you can specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on devices will be logged to either the audit or shadow log. Use the left mouse button to select days and hours when the selected user's actions on devices will be logged. Use the right mouse button to mark days and hours when the selected user's actions on devices will not be logged*.
To change audit and shadowing rules for an existing user or group	1. In the upper-left pane of the dialog box, under **Users**, select the user or group. 2. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate audit and shadowing rights.
To remove an existing user or group and rules	• In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key. *When you remove a user or group, any rules for that user or group will also be removed*.

6. Click **OK** or **Apply**.

Enabling Offline Alerts

Offline alerts for specific access-related events are enabled in the **Auditing, Shadowing & Alerts (Offline)** dialog box. Enabling offline alerts is similar to defining offline audit rules and includes the following basic steps:

- Specify which events will trigger alert notifications. You can enable notification of successful and/ or failed attempts to access a device. Select the **Alert Allowed** check box to enable notification of successful attempts to access a device. Select the **Alert Denied** check box to enable notification of failed attempts to access a device.
- Specify users and/or groups whose actions will trigger alert notifications. To do so, in the upper-left pane of the dialog box, under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.
- Specify which user's actions on devices either will or will not trigger alert notifications. In the upper-left pane of the dialog box, under **Users**, select the user or group that you added. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny an alert right. Alert rights determine which user actions on devices trigger alert notifications. Alert rights are identical to audit rights. The only difference is that when events matching specific criteria occur DeviceLock triggers alerts instead of logging these events in the Audit Log. For detailed information on Audit rights for devices, see "Auditing, Shadowing & Alerts (Regular Profile)."
- Specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on devices either will or will not trigger alert notifications. To do so, in the right pane of the dialog box, use the left mouse button to select days and hours when the selected user's actions on devices will trigger alert notifications. Use the right mouse button to mark days and hours when the selected user's actions on devices will not trigger alert notifications.

Undefining Offline Audit and Shadowing Rules

You can return previously defined offline audit and shadowing rules to the unconfigured state. If offline rules are undefined, regular rules are applied to offline client computers.

To undefine offline audit and shadowing rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, select **Auditing, Shadowing & Alerts**.

   When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view device types for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each device type in the Offline column.

4. In the details pane, right-click the device type for which you want to undefine offline audit and shadowing rules, and then click **Undefine Offline**.

   You can undefine audit and shadowing rules defined for several device types at the same time. To do this, do the following:

   a) In the details pane, select several device types by holding down the SHIFT key or the CTRL key while clicking them.
   b) Right-click the selection, and then click **Undefine Offline**.
   The offline state of the audit and shadowing rules changes to "Not Configured."

Removing Offline Audit and Shadowing Rules

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of higher-level offline audit and shadowing rules and enforce regular audit and shadowing rules on specific lower-level groups of client computers. To enforce regular audit and shadowing rules, you must remove offline audit and shadowing rules.

To remove offline audit and shadowing rules

1. If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, select **Auditing, Shadowing & Alerts**.

   When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view device types for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each device type in the Offline column.

4. In the details pane, right-click the device type for which you want to remove offline audit and shadowing rules, and then click **Remove Offline**.

You can remove audit and shadowing rules defined for several device types at the same time. To do this, do the following:

a) In the details pane, select several device types by holding down the SHIFT key or the CTRL key while clicking them.
b) Right-click the selection, and then click **Remove Offline**.

The offline state of the audit and shadowing rules changes to "Use Regular."

The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline USB Devices White List

For a detailed description of the USB Devices White List feature, see "USB Devices White List (Regular Profile)."

The offline USB Devices White List can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that the white list is not defined. The following message is displayed: "Offline USB White List is not configured." This is the default state.
Configured	Indicates that the white list is defined.
Use Regular	Indicates that the inheritance of the offline white list is blocked and the regular white list is enforced. Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of the regular white list is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of the regular white list lets you prevent the offline white list inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of the regular white list, see "Removing Offline USB Devices White List."

Managing the offline USB Devices White List involves the following tasks:

- Defining and editing the offline USB Devices White List
- Exporting and importing the offline USB Devices White List
- Undefining the offline USB Devices White List
- Removing the offline USB Devices White List

Defining and Editing Offline USB Devices White List

To define and edit the offline USB Device White List

1. If you use DeviceLock Management Console, do the following:

a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Service Settings Editor, do the following:

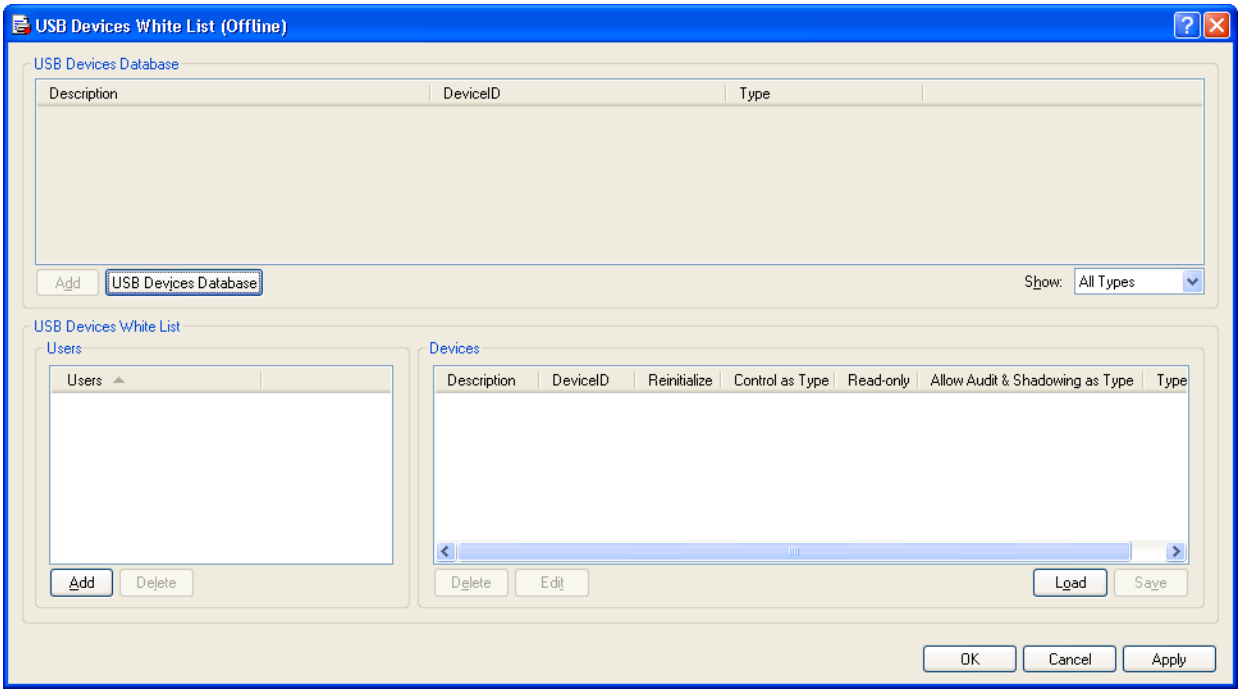
a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

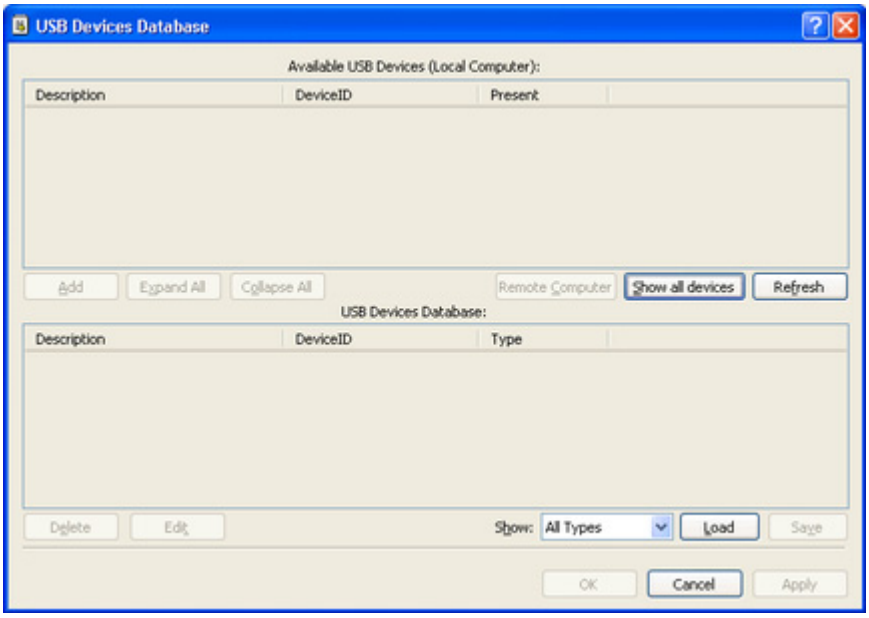
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **USB Devices White List**, and then click **Manage Offline**.
     - OR -
   - Select **USB Devices White List**, and then click **Manage Offline** on the toolbar.

The USB Devices White List (Offline) dialog box appears.



4. In the upper pane of the **USB Devices White List (Offline)** dialog box, under **USB Devices Database**, click **USB Devices Database**.

The USB Devices Database dialog box appears.



In the upper pane of the USB Devices Database dialog box, under Available USB Devices, you can view the devices that are currently plugged in.

To view all devices ever plugged into USB ports on the computer, click **Show all devices**. To view available devices on a remote computer, click **Remote Computer**.

The Remote Computer button is unavailable when the management console is connected to the local computer.

5. In the upper pane of the **USB Devices Database** dialog box, under **Available USB Devices**, select the device you want to add to the USB Devices White List, and then click **Add**.

   The device that you added is displayed under USB Devices Database in the lower pane of the dialog box.

   Note: You can add a device to the USB Devices White List only after you add this device to the USB Devices Database.

   The same USB Devices Database is used for both the regular and offline USB Devices White List.

   To delete a device from the USB Devices Database, in the lower pane of the **USB Devices Database** dialog box, under **USB Devices Database**, do one of the following:

   - Select the device, and then click **Delete**.
     - OR -
   - Right-click the device, and then click **Delete**.

   Devices are not deleted automatically from the white list after you delete them from the USB Devices Database.

   To edit a device's description, in the lower pane of the **USB Devices Database** dialog box, under **USB Devices Database**, select the device, and then click **Edit**.

If you change a device's description in the USB Database, the following behavior occurs: The device will have its old description in the white list if it has already been added to the white list.

6. Click **OK** or **Apply**.

   The device that you added to the USB Devices Database is displayed under USB Devices Database in the upper pane of the USB Devices White List (Offline) dialog box.

7. In the lower-left pane of the **USB Devices White List (Offline)** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

8. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the USB Devices White List, and then click **OK**.

   The users and groups that you added are displayed under Users in the lower-left pane of the USB Devices White List (Offline) dialog box.

   To delete a user or group, in the lower-left pane of the **USB Devices White List (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

9. In the lower-left pane of the **USB Devices White List (Offline)** dialog box, under **Users**, select the user or group.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

10. In the upper pane of the **USB Devices White List (Offline)** dialog box, under **USB Devices Database**, select the device you want to add to the white list for the selected user or group, and then click **Add**.

    You can select multiple devices by holding down the SHIFT key or the CTRL key while clicking them.

    The devices that you added to the white list are displayed under Devices in the lower-right pane of the dialog box.

    To delete a device from the white list for the selected user or group, in the lower-right pane of the **USB Devices White List (Offline)** dialog box, under **Devices**, do the following:

    - Select the device, and then click **Delete**.
      - OR -
    - Right-click the device, and then click **Delete**.
      - OR -
    - Select the device, and then press the DELETE key.

    To edit a device's description, in the lower-right pane of the **USB Devices White List (Offline)** dialog box, under **Devices**, do the following:

    - Select the device, and then click **Edit**.
      - OR -
    - Right-click the device, and then click **Edit**.

11. Click **OK** or **Apply**.

Exporting and Importing Offline USB Devices White List

You can export the offline USB Devices White List to a .whl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

To export the offline USB Devices White List

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **USB Devices White List**, and then click **Save Offline**.
     - OR -
   - Select **USB Devices White List**, and then click **Save Offline** on the toolbar.
     - OR -
   - Expand **USB Devices White List**, right-click any user or group specified in the white list, and then click **Save Offline**.
     - OR -
   - Expand **USB Devices White List**, select any user or group specified in the white list. In the details pane, right-click the white listed device, and then click **Save**.
     - OR -
   - Right-click **USB Devices White List**, and then click **Manage Offline**. In the lower-right pane of the **USB Devices White List (Offline)** dialog box, under **Devices**, click **Save**.

   The Save As dialog box appears.
4. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the .whl file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.

   When you export the offline USB Devices White List, it is saved in a file with a .whl extension.

To import the offline USB Devices White List

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **USB Devices White List**, and then click **Load Offline**.
     - OR -
   - Select **USB Devices White List**, and then click **Load Offline** on the toolbar.
     - OR -
   - Expand **USB Devices White List**, right-click any user or group specified in the white list, and then click **Load Offline**.
     - OR -
   - Expand **USB Devices White List**, and then select any user or group specified in the white list. In the details pane, right-click the white listed device, and then click **Load**.
     - OR -
   - Right-click **USB Devices White List**, and then click **Manage Offline**. In the lower-right pane of the **USB Devices White List (Offline)** dialog box, under **Devices**, click **Load**.

   The Open dialog box appears.
4. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
5. In the folder list, locate and open the folder that contains the file.
6. Click the file, and then click **Open**.

Undefining Offline USB Devices White List

You can return the previously defined offline white list to the unconfigured state. If the offline white list is undefined, the regular white list is applied to offline client computers.

To undefine the offline USB Devices White List

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.

b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, right-click **USB Devices White List**, and then click **Undefine Offline**.

   The offline state of the white list changes to "Not Configured."

   When you select **USB Devices White List** in the console tree, in the details pane the following message is displayed: "Offline USB White List is not configured."

Removing Offline USB Devices White List

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of the higher-level offline white list and enforce the regular white list on specific lower-level groups of client computers. To enforce the regular USB Devices White List, you must remove the offline USB Devices White List.

To remove the offline USB Devices White List

1. If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, right-click **USB Devices White List**, and then click **Remove Offline**.

   The offline state of the white list changes to "Use Regular."

   When you select **USB Devices White List** in the console tree, in the details pane the following message is displayed: "Offline USB White List is configured to use Regular USB White List.

   The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline Media White List

For a detailed description of the Media White List feature, see "Media White List (Regular Profile)."

The offline Media White List can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that the white list is not defined. The following message is displayed: "Offline Media White List is not configured." This is the default state.
Configured	Indicates that the white list is defined.
Use Regular	Indicates that the inheritance of the offline white list is blocked and the regular white list is enforced. Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of the regular white list is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of the regular white list lets you prevent the offline white list inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of the regular white list, see "Removing Offline Media White List."

Managing the offline Media White List involves the following tasks:

- Defining and editing the offline Media White List
- Exporting and importing the offline Media White List
- Undefining the offline Media White List
- Removing the offline Media White List

Defining and Editing Offline Media White List

To define and edit the offline Media White List

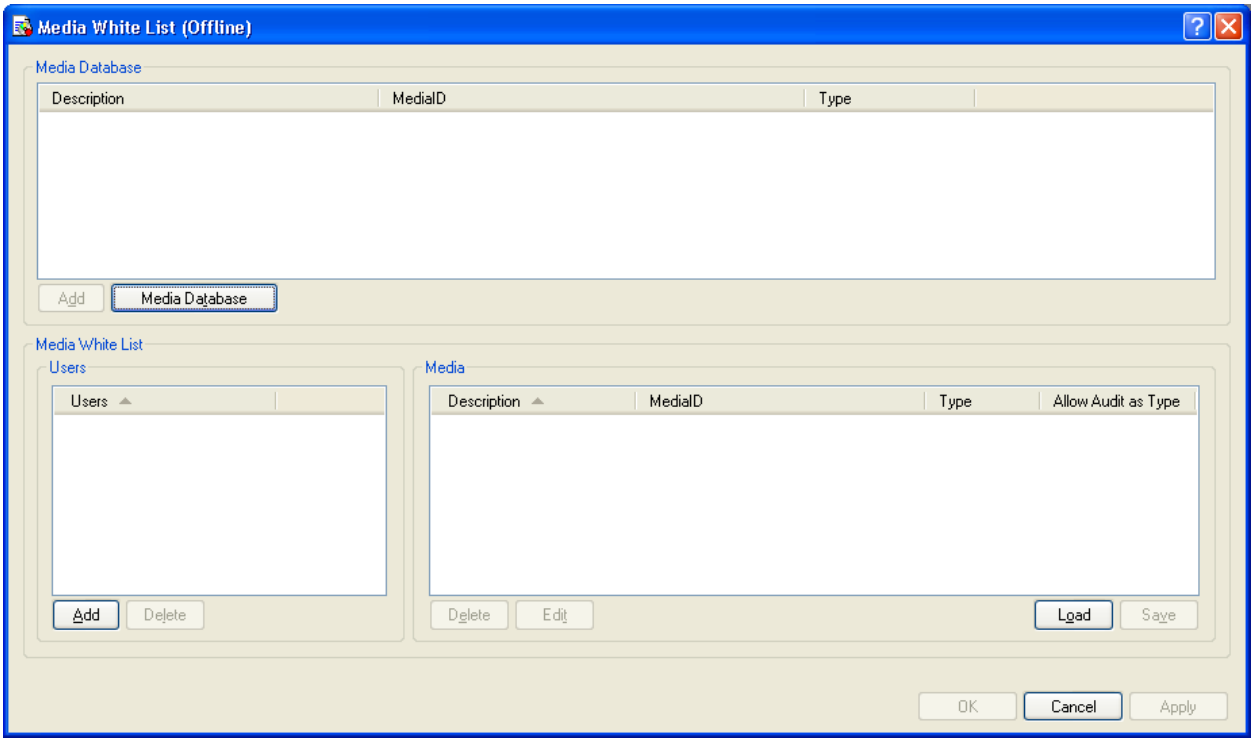
1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

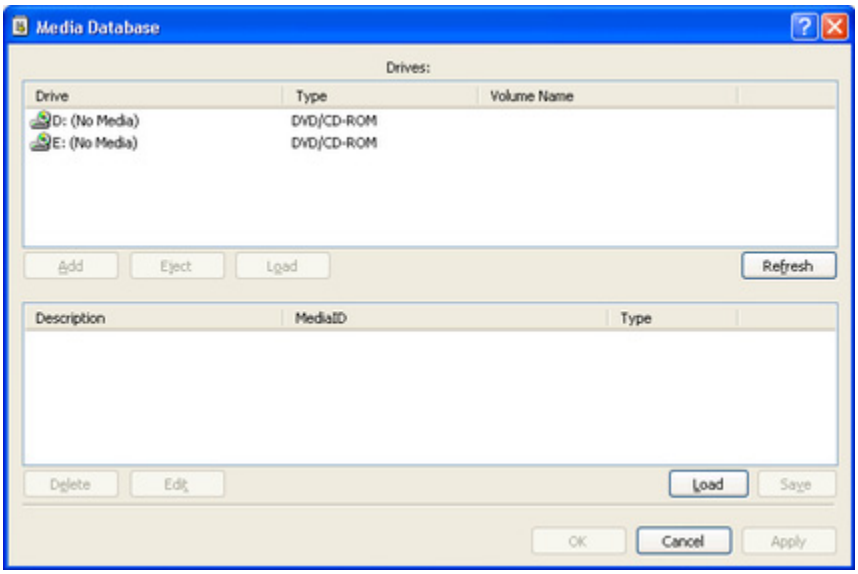
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Media White List**, and then click **Manage Offline**.
     - OR -
   - Select **Media White List**, and then click **Manage Offline** on the toolbar.

   The Media White List (Offline) dialog box appears.



4. In the upper pane of the **Media White List (Offline)** dialog box, under **Media Database**, click **Media Database**.

   The Media Database dialog box appears.



In the upper pane of the Media Database dialog box, under Drives, you can view all CD/DVD/BD-ROM drives available on the local computer.

*The list of drives is automatically refreshed and displays new media as soon as they arrive. To manually refresh this list, click **Refresh**.*

5. In the upper pane of the **Media Database** dialog box, under **Drives**, select the drive that contains the media you want to add to the Media White List, and then click **Add**.

   The selected media are added to the Media Database and can be viewed in the lower pane of the Media Database dialog box.

   Note: You can add media to the Media White List only after you add the media to the Media Database.

   The same Media Database is used for both the regular and offline Media White List.

   To delete a medium from the white list, in the lower pane of the **Media Database** dialog box, do the following:

   - Select the medium, and then click **Delete**.
     - OR -
   - Right-click the medium, and then click **Delete**.

   To edit a medium's description, in the lower pane of the **Media Database** dialog box, select the medium, and then click **Edit**.

6. Click **OK** or **Apply**.

   The media that you added to the Media Database are displayed under Media Database in the upper pane of the Media White List (Offline) dialog box.

7. In the lower-left pane of the **Media White List (Offline)** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

8. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the Media White List, and then click **OK**.

The users and groups that you added are displayed under Users in the lower-left pane of the Media White List (Offline) dialog box.

To delete a user or group, in the lower-left pane of the **Media White List (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

9. In the lower-left pane of the **Media White List (Offline)** dialog box, under **Users**, select the user or group.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

10. In the upper pane of the **Media White List (Offline)** dialog box, under **Media Database**, select the medium you want to add to the white list for the selected user or group, and then click **Add**.

    You can select multiple media by holding down the SHIFT key or the CTRL key while clicking them.

    The media that you added to the white list are displayed under Media in the lower-right pane of the dialog box.

    To delete a medium from the white list for the selected user or group, in the lower-right pane of the **Media White List (Offline)** dialog box, under **Media**, do the following:

    - Select the medium, and then click **Delete**.
      - OR -
    - Right-click the medium, and then click **Delete**.

    To edit a medium's description for the selected user or group, in the lower-right pane of the **Media White List (Offline)** dialog box, under **Media**, do the following:

    - Select the medium, and then click **Edit**.
      - OR -
    - Right-click the medium, and then click **Edit**.

11. Click **OK** or **Apply**.

Exporting and Importing Offline Media White List

You can export the offline Media White List to a .mwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

To export the offline Media White List

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Media White List**, and then click **Save Offline**.
     - OR -
   - Select **Media White List**, and then click **Save Offline** on the toolbar.
     - OR -
   - Expand **Media White List**, right-click any user or group specified in the white list, and then click **Save Offline**.
     - OR -
   - Expand **Media White List**, and then select any user or group specified in the white list. In the details pane, right-click the white listed medium, and then click **Save**.
     - OR -
   - Right-click **Media White List**, and then click **Manage Offline**. In the lower-right pane of the **Media White List (Offline)** dialog box, under **Media**, click **Save**.

   The Save As dialog box appears.
4. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the .mwl file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.

   When you export the offline Media White List, it is saved in a file with a .mwl extension.

To import the offline Media White List

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Media White List**, and then click **Load Offline**.

- OR -

- Select **Media White List**, and then click **Load Offline** on the toolbar.

- OR -

- Expand **Media White List**, right-click any user or group specified in the white list, and then click **Load Offline**.

- OR -

- Expand **Media White List**, and then select any user or group specified in the white list. In the details pane, right-click the white listed device, and then click **Load**.

- OR -

- Right-click **Media White List**, and then click **Manage Offline**. In the lower-right pane of the **Media White List (Offline)** dialog box, under **Media**, click **Load**.

The Open dialog box appears.

4. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
5. In the folder list, locate and open the folder that contains the file.
6. Click the file, and then click **Open**.

Undefining Offline Media White List

You can return the previously defined offline white list to the unconfigured state. If the offline white list is undefined, the regular white list is applied to offline client computers.

To undefine the offline Media White List

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, right-click **Media White List**, and then click **Undefine Offline**.

   The offline state of the white list changes to "Not Configured."

   When you select **Media White List** in the console tree, in the details pane the following message is displayed: "Offline Media White List is not configured."

Removing Offline Media White List

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of the higher-level offline white list and enforce the regular white list on specific lower-level groups of client computers. To enforce the regular Media White List, you must remove the offline Media White List.

To remove the offline Media White List

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, right-click **Media White List**, and then click **Remove Offline**.

   The offline state of the white list changes to "Use Regular."

   When you select **Media White List** in the console tree, in the details pane the following message is displayed: "Offline Media White List is configured to use Regular Media White List.

   The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline Content-Aware Rules for Devices

For a detailed description of the Content-Aware Rules feature for devices, see "Content-Aware Rules for Devices (Regular Profile)."

The offline Content-Aware Rules can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that Content-Aware Rules are not defined. The following message is displayed: "Offline Content-Aware Rules are not configured." This is the default state.
Configured	Indicates that Content-Aware Rules are defined.
Use Regular	Indicates that the inheritance of offline Content-Aware Rules is blocked and regular Content-Aware Rules are enforced. Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of regular Content-Aware Rules is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of regular Content-Aware Rules lets you prevent offline Content-Aware Rules inherited from a higher level from being

STATE	DESCRIPTION
	applied to a specific group of client computers at a lower level. For more information on the enforcement of regular Content-Aware Rules, see "Removing Offline Content-Aware Rules."

Managing offline Content-Aware Rules involves the following tasks:

- Defining offline Content-Aware Rules
- Editing offline Content-Aware Rules
- Copying offline Content-Aware Rules
- Exporting and importing offline Content-Aware Rules
- Deleting offline Content-Aware Rules
- Undefining offline Content-Aware Rules
- Removing offline Content-Aware Rules

Defining Offline Content-Aware Rules

Content-Aware Rules are created based on either the built-in or custom content groups. For detailed information on these groups, see "Configuring Content Detection Settings."

You can enable offline alerts that are sent when a specific offline Content-Aware Rule fires. Such alerts are enabled at the time you define an offline Content-Aware Rule.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific Content-Aware Rule, you must configure alert settings in **Service Options**.

To define an offline Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

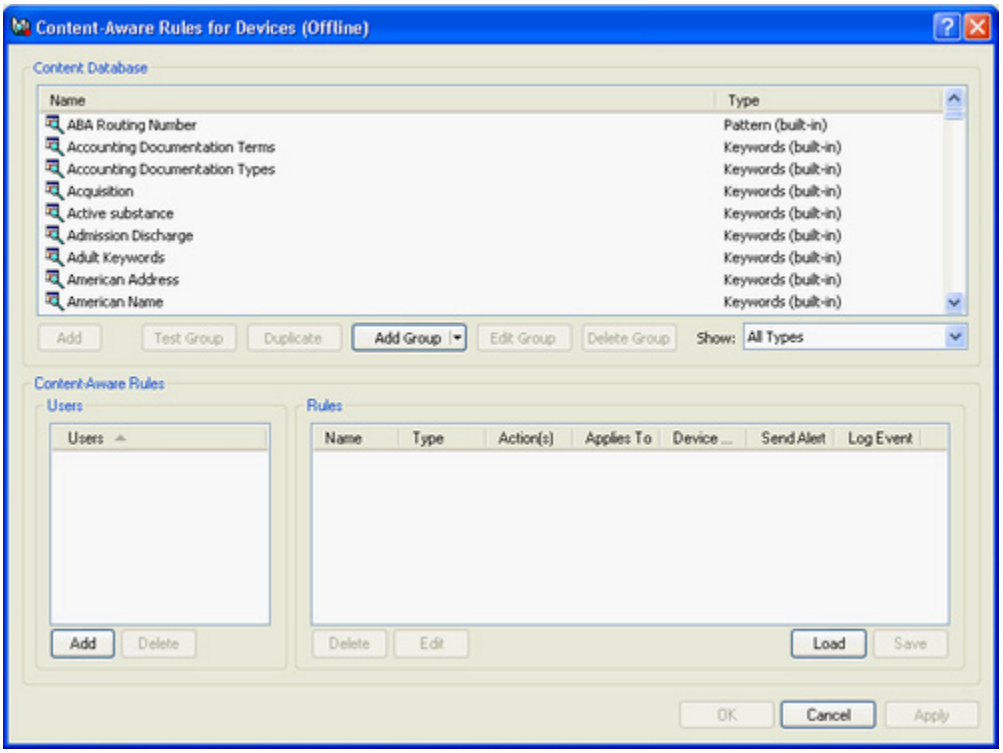
   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage Offline**.

- OR -

- Select **Content-Aware Rules**, and then click **Manage Offline** on the toolbar.

The Content-Aware Rules for Devices (Offline) dialog box appears.



4. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Devices (Offline) dialog box.

   To delete a user or group, in the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

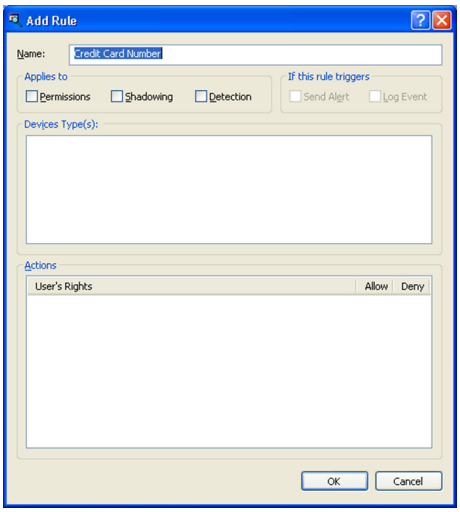
6. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the users or groups for which you want to define the rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

7. In the upper pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Content Database**, select the desired content group, and then click **Add**.

Note: You can specify only one content group for a Content-Aware Rule.

The Add Rule dialog box appears.



8. In the **Add Rule** dialog box, in the **Name** box, type the name of the Content-Aware Rule.

   By default, the Content-Aware Rule has the same name as the specified content group but you can enter a different name.

9. Under **Applies to**, specify the type of operation associated with the rule. The available options are:

   - **Permissions**: Specifies that the rule will apply to access control operations.
   - **Shadowing**: Specifies that the rule will apply to shadow copy operations.
   - **Detection**: Specifies that the rule will apply to detection operations.
   - **Permissions**, **Shadowing**: Specifies that the rule will apply to both access control and shadow copy operations.
   - **Permissions, Detection**: Specifies that the rule will apply to both access control and detection operations.
   - **Shadowing, Detection**: Specifies that the rule will apply to both shadow copy and detection operations.
   - **Permissions, Shadowing, Detection**: Specifies that the rule will apply to all available operations: access control, shadow copy, and detection.

10. Under **If this rule triggers**, specify the following additional actions to be performed when the rule triggers:

    - **Send Alert**: Specifies that an alert is sent whenever the rule triggers.
    - **Log Event**: Specifies that an event is logged in the Audit Log whenever the rule triggers.

11. Under **Device Type(s)**, select the appropriate device type(s) you would like this rule to be applied to.

    Content-Aware Rules can be applied to the following device types: Clipboard, Floppy, iPhone, MTP, Optical Drive, Palm, Printer, Removable, TS Devices, and Windows Mobile.

12. Under **Action(s)**, specify which user actions are allowed or disallowed on files, which user actions are logged to the shadow log, and which user actions are detected.

    If the rule applies to shadow copy operations combined with other operations, the Read user right becomes unavailable. If the rule applies to detection operations combined with other operations, only Allow action becomes available. For detailed information on user rights and actions that can be specified in Content-Aware Rules, see "Content-Aware Rules for Access Control Operations", "Content-Aware Rules for Shadow Copy Operations" and "Content-Aware Rules for Detection Operations".

13. Click **OK**.

    The rule you created is displayed under Rules in the lower-right pane of the Content-Aware Rules for Devices (Offline) dialog box.

14. Click **OK** or **Apply** to apply the rule.

    The users or groups to which the Content-Aware Rule applies are displayed under Content-Aware Rules in the console tree.

    When you select a user or group to which a Content-Aware Rule applies in the console tree, in the details pane you can view detailed information regarding this rule. This information includes the following:

    - **Name** The name of the rule. By default, the rule has the same name as the specified content group.
    - **Type** The type of the content analysis. Possible values: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties**, **Complex** and **Oracle IRM**. **File Type Detection** indicates that recognition and identification of files is based on their characteristic signatures. **Keywords** indicates that recognition and identification of data/files is based on the specified keywords or phrases. **Pattern** indicates that recognition and identification of data/files is based on the specified patterns of text described by Perl regular expressions. **Document Properties** indicates that recognition and identification of files is based on their properties. **Complex** indicates that recognition and identification of data/files is based on the specified content described by a Boolean expression. **Oracle IRM** indicates that recognition and identification of files is based on their IRM contexts.
    - **Action(s)** Shows which user actions are allowed or disallowed on files and which user actions are logged to the shadow log.
    - **Applies To** Possible values: **Permissions**, **Shadowing**, **Detection**, **Permissions+Shadowing, Permissions+Detection, Shadowing+Detection, Permissions+Shadowing+Detection**. **Permissions** indicates that the rule applies to access control operations. **Shadowing** indicates that the rule applies to shadow copy operations.**Detection** indicates that the rule applies to detection operations. **Permissions+Shadowing** indicates that the rule applies to both access control and shadow copy operations. **Permissions+Detection** indicates that the rule applies to both access control and detection operations. **Shadowing+Detection** indicates that the rule applies to both shadow copy and detection operations. **Permissions+Shadowing+Detection** indicates that the rule applies to all available operations: access control, shadow copy, and detection.
    - **Device Type(s)** The device type(s) to which the rule applies.
    - **Send Alert** Shows whether alerts are enabled or disabled for this rule.

- **Log Event** Shows whether audit logging of events associated with this rule is enabled or disabled.
- **Profile** Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to computers that are working offline.
  You can define different online vs. offline Content-Aware Rules for the same user or sets of users. For information about how to define online Content-Aware Rules, see "Managing Content-Aware Rules."

Editing Offline Content-Aware Rules

You can modify the Content-Aware Rule properties such as **Name**, **Applies To**, **If this rule triggers**, **Device Type(s)**, **Actions**.

To edit an offline Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, right-click **Content-Aware Rules**, click **Manage Offline**, and then do the following:
   a) In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the user or group for which you want to edit the rule.
   By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.
   b) In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.
   - OR -
   Right-click the rule, and then click **Edit**.

   - OR -

   Under **Devices**, expand **Content-Aware Rules**, and then do the following:
   a) Under **Content-Aware Rules**, select the user or group for which you want to edit the rule.
   By selecting users or groups, you can view the Content-Aware Rules applied to them in the details pane.

b) In the details pane, right-click the rule you want to edit, and then click **Edit**.

The Edit Rule dialog box appears.

4. In the **Edit Rule** dialog box, modify the rule properties as required to meet your needs.
5. Click **OK** to apply the changes.

Copying Offline Content-Aware Rules

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing offline Content-Aware Rules.

To copy an offline Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage Offline**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage Offline** on the toolbar.

   The Content-Aware Rules for Devices (Offline) dialog box appears.
4. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.

   By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.
5. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

   The rule you cut or copy is automatically copied to the Clipboard.

   You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you cut the rule, the rule will be cut only after you paste it.

   To perform a drag-and-drop operation, select the rule and move it to the user or group to which you want to apply the copied rule.

6. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Devices (Offline) dialog box.

8. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the users or groups for which you want to set permissions.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

9. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, right-click in the **Rules** pane and then click **Paste**.

   The copied rule is displayed under Rules in the lower-right pane of the Content-Aware Rules for Devices (Offline) dialog box.

10. Click **OK** or **Apply** to apply the copied rule.

Exporting and Importing Offline Content-Aware Rules

You can export all your current offline Content-Aware Rules to a .cwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

To export offline Content-Aware Rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Save Offline**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Save Offline** on the toolbar.

- OR -

- Expand **Content-Aware Rules**, right-click any user or group, and then click **Save Offline**.

  - OR -

- Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Save**.

  - OR -

- Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Save Offline** on the toolbar.

  - OR -

- Right-click **Content-Aware Rules**, and then click **Manage (Offline)**. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Rules**, click **Save**.

The Save As dialog box appears.

4. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the .cwl file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.

   When you export rules, they are saved in a file with a .cwl extension.

To import offline Content-Aware Rules

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, do one of the following:

   - Right-click **Content-Aware Rules**, and then click **Load Offline**.

     - OR -

   - Select **Content-Aware Rules**, and then click **Load Offline** on the toolbar.

     - OR -

   - Expand **Content-Aware Rules**, right-click any user or group, and then click **Load Offline**.

     - OR -

- Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Load**.

  - OR -

- Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Load Offline** on the toolbar.

  - OR -

- Right-click **Content-Aware Rules**, and then click **Manage Offline**. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Rules**, click **Load**.

The Open dialog box appears.

4. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
5. In the folder list, locate and open the folder that contains the file.
6. Click the file, and then click **Open**.

   You can import only one .cwl file at a time.

Deleting Offline Content-Aware Rules

You can delete individual offline Content-Aware Rules when they are no longer required.

To delete an offline Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, do one of the following:

   - Expand **Content-Aware Rules**, right-click the user or group to which the rule is applied, and then click **Delete user**.

     When you delete a user or group, the rule associated with this user or group is automatically deleted.

     - OR -

   - Expand **Content-Aware Rules**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.

     - OR -

- Right-click **Content-Aware Rule**s, and then click **Manage Offline**. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the user or group to which the rule is applied. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.

  You can select multiple rules that you want to delete by holding down the SHIFT key or the CTRL key while clicking them.

Undefining Offline Content-Aware Rules

You can return the previously defined offline Content-Aware Rules to the unconfigured state. If offline rules are undefined, regular rules are applied to offline client computers.

To undefine offline Content-Aware Rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, right-click **Content-Aware Rules**, and then click **Undefine Offline**.

   The offline state of Content-Aware Rules changes to "Not Configured."

   When you select **Content-Aware Rules** in the console tree, in the details pane the following message is displayed: "Offline Content-Aware Rules are not configured."

Removing Offline Content-Aware Rules

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of higher-level offline Content-Aware Rules and enforce regular Content-Aware Rules on specific lower-level groups of client computers. To enforce regular Content-Aware Rules, you must remove offline Content-Aware Rules.

To remove offline Content-Aware Rules

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, right-click **Content-Aware Rules**, and then click **Remove Offline**.

   The offline state of Content-Aware Rules changes to "Use Regular."

   When you select **Content-Aware Rules** in the console tree, in the details pane the following message is displayed: "Offline Content-Aware Rules are configured to use Regular Content-Aware Rules."

   The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline Security Settings

For a detailed description of the Security Settings feature, see "Security Settings (Regular Profile)."

Offline Security Settings can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that Security Settings are not defined. This is the default state.
Enabled	Indicates that Security Settings are defined to enable audit and access control for the specified device classes.
Disabled	Indicates that Security Settings are defined to disable audit and access control for the specified device classes.
Use Regular	Indicates that the inheritance of offline Security Settings is blocked and regular Security Settings are enforced. Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of regular Security Settings is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of regular Security Settings lets you prevent offline Security Settings inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of regular Security Settings, see "Removing Offline Security Settings."

Managing offline Security Settings involves the following tasks:

- Defining and changing offline Security Settings
- Undefining offline Security Settings
- Removing offline Security Settings

Defining and Changing Offline Security Settings

Offline Security Settings can be defined and changed individually or collectively.

To define and change offline Security Settings individually

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Security Settings**.

   When you select Security Settings in the console tree, they are displayed in the details pane.
4. In the details pane, right-click any Security Setting, and then click **Enable Offline**.

   The Security Setting changes its offline state from "Not Configured" to "Enabled."

   Once you have enabled a particular Security Setting, you can disable it. To do so, right-click the enabled Security Setting, and then click **Disable Offline**.

   The Security Setting changes its offline state from "Enabled" to "Disabled."

To define and change offline Security Settings collectively

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
   - Right-click **Security Settings**, and then click **Manage Offline**.

- OR –

- Select **Security Settings**, and then click **Manage Offline** on the toolbar.

- OR -

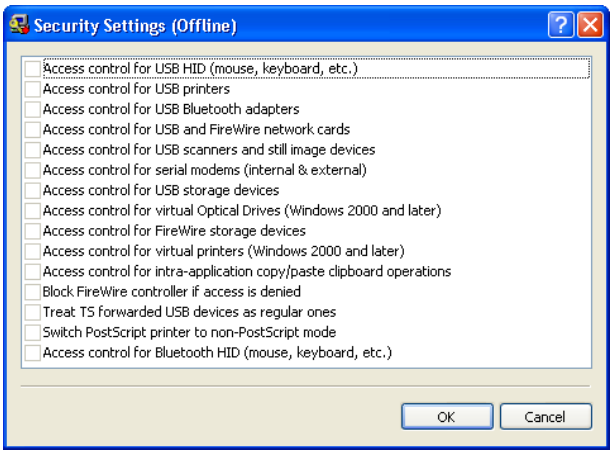
- Select **Security Settings**. In the details pane, right-click any Security Setting, and then click **Manage Offline.**

- OR –

- Select **Security Settings**. In the details pane, select any Security Setting, and then click **Manage Offline** on the toolbar.

  When you select Security Settings in the console tree, they are displayed in the details pane.

The Security Settings (Offline) dialog box appears.


Security Settings (Offline)
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB Bluetooth adapters
Access control for USB and FireWire network cards
Access control for USB scanners and still image devices
Access control for serial modems (internal & external)
Access control for USB storage devices
Access control for virtual Optical Drives (Windows 2000 and later)
Access control for FireWire storage devices
Access control for virtual printers (Windows 2000 and later)
Access control for intra-application copy/paste clipboard operations
Block FireWire controller if access is denied
Treat TS forwarded USB devices as regular ones
Switch PostScript printer to non-PostScript mode
Access control for Bluetooth HID (mouse, keyboard, etc.)
OK
Cancel

4. In the **Security Settings (Offline)** dialog box, select the appropriate check boxes for the Security Settings that you want to define.

   Once you have enabled Security Settings, you can disable them. To do so, clear the appropriate check boxes.

   Note: All check boxes in the **Security Settings (Offline)** dialog box have three states: selected, cleared, and indeterminate that correspond to the Enabled, Disabled, and Not Configured states of Security Settings.

5. Click **OK**.

Undefining Offline Security Settings

You can return the previously defined offline Security Settings to the unconfigured state. If offline Security Settings are undefined, regular Security Settings are applied to offline client computers. You can undefine Security Settings individually or collectively.

To undefine offline Security Settings individually

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.

   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, select **Security Settings**.

   When you select Security Settings in the console tree, they are displayed in the details pane.

4. In the details pane, right-click any Security Setting you want to undefine, and then click **Undefine Offline**.

   The Security Setting changes its offline state to "Not Configured."

To undefine offline Security Settings collectively

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Devices**.
3. Under **Devices**, do one of the following:

   - Right-click **Security Settings**, and then click **Manage Offline**.
     - OR –
   - Select **Security Settings**, and then click **Manage Offline** on the toolbar.
     - OR -
   - Select **Security Settings**. In the details pane, right-click any Security Setting, and then click **Manage Offline.**
     - OR –
   - Select **Security Settings**. In the details pane, select any Security Setting, and then click **Manage Offline** on the toolbar.
     When you select Security Settings in the console tree, they are displayed in the details pane.

   The Security Settings (Offline) dialog box appears.

4. In the **Security Settings (Offline)** dialog box, return the appropriate check boxes to the indeterminate state.

> **Note:** All check boxes in the **Security Settings (Offline)** dialog box have three states: selected, cleared, and indeterminate that correspond to the Enabled, Disabled, and Not Configured states of Security Settings.

Removing Offline Security Settings

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of higher-level offline Security Settings and enforce regular Security Settings on specific lower-level groups of client computers. To enforce regular Security Settings, you must remove offline Security Settings. You can remove only individual Security Settings.

To remove offline Security Settings

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Security Settings**.

   When you select Security Settings in the console tree, they are displayed in the details pane.
4. In the details pane, right-click any Security Setting you want to remove, and then click **Remove Offline**.

   The Security Setting changes its offline state to "Use Regular."

   The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline Security Policies for Protocols

Managing offline security policies for protocols involves the following operations:

- Managing offline Permissions for protocols
- Managing offline audit, shadowing rules and alerts for protocols
- Managing offline Protocols White List
- Managing offline IP Firewall
- Managing offline Content-Aware Rules for protocols
- Managing offline Security Settings for protocols

Managing Offline Permissions for Protocols

For a detailed description of the Permissions feature for protocols, see "Managing Permissions for Protocols."

Offline permissions can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that permissions on a protocol are not set. This is the default state.
Configured	Indicates that permissions on a protocol are set.
Full Access	Indicates that full access rights are granted to the Everyone account.
No Access	Indicates one of the following: • The Everyone account has No Access permissions and is the only account assigned to a protocol. *No Access permissions assigned to the Everyone account take priority over permissions assigned to other accounts*. • All users and groups assigned to a protocol have No Access permissions. • All users and groups assigned to a protocol are removed.
Use Regular	Indicates that the inheritance of offline permissions is blocked and regular permissions are enforced. Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of regular permissions is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of regular permissions lets you prevent offline permissions inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of regular permissions, see "Removing Offline Permissions."

Managing offline permissions involves the following tasks:

- Setting and editing offline permissions
- Undefining offline permissions
- Removing offline permissions

Setting and Editing Offline Permissions

To set and edit offline permissions

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

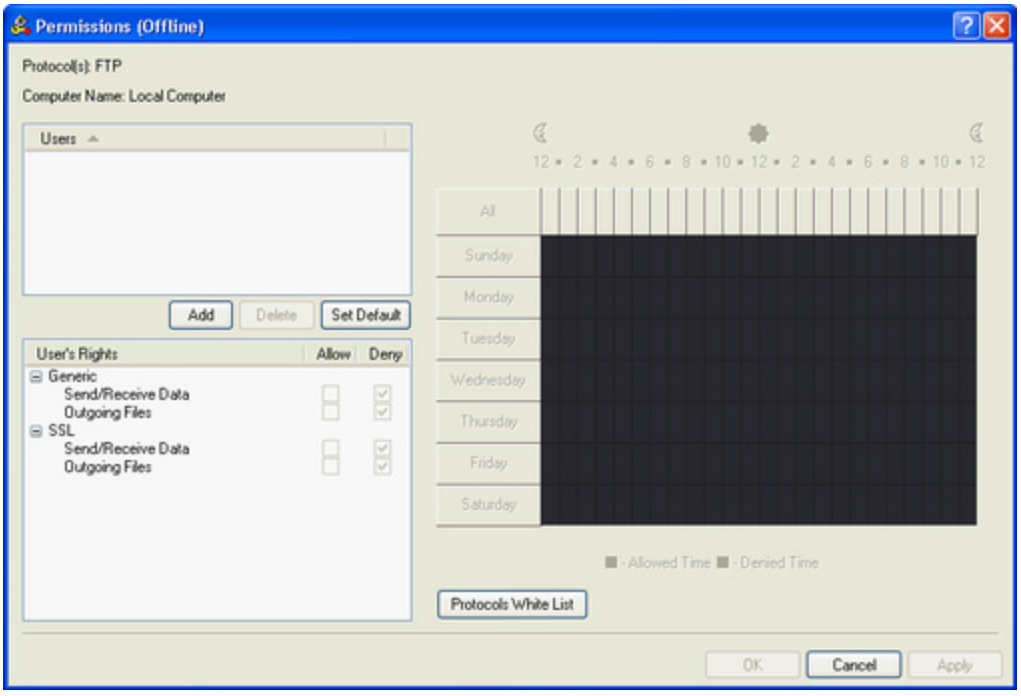
2. Expand **Protocols**.
3. Under **Protocols**, select **Permissions**.

   When you select Permissions in the console tree, in the details pane you can view protocols for which you can set permissions. In the details pane, you can also view the current state of offline permissions for each protocol in the Offline column.

4. In the details pane, do one of the following:

   - Right-click the protocol for which you want to set or edit permissions, and then click **Set Offline Permissions**.
     - OR -
   - Select the protocol for which you want to set or edit permissions, and then click **Set Offline Permissions** on the toolbar.

   The Permissions (Offline) dialog box appears.



5. In the **Permissions (Offline)** dialog box, do the following:

TO DO THIS	FOLLOW THESE STEPS
To set the default permissions	• In the upper-left pane of the dialog box, under **Users**, click **Set Default**. *The default permissions are assigned to the Administrators and*

TO DO THIS	FOLLOW THESE STEPS
	Everyone accounts. For information about which permissions are set for these accounts by default, see "Managing Permissions for Protocols."
To set permissions for an additional user or group	1. In the upper-left pane of the dialog box, under **Users**, click **Add**. *The Select Users or Groups dialog box appears.* 2. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**. *The users and groups that you added are* displayed *under Users in the upper-left pane of the Permissions (Offline) dialog box*. 3. In the upper-left pane of the **Permissions (Offline)** dialog box, under **Users**, select the user or group. *You can select multiple users and/ or groups by holding down the SHIFT key or the CTRL key while clicking them*. 4. In the lower-left pane of the **Permissions (Offline)** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate access rights. *In the right pane of the Permissions (Offline) dialog box, you can set day and time restrictions that narrow user access to the specified protocol(s). Use the left mouse button to select days and hours when the selected user or group will have access to the specified protocol(s). Use the right mouse button to mark days and hours when the selected user or group will not have access to the specified protocol(s).*
To change permissions for an existing user or group	1. In the upper-left pane of the dialog box, under **Users**, select the user or group. 2. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate access rights.
To remove an existing user or group and permissions	• In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key. *When you remove a user or group, any permissions for that user or group will also be removed*.

6. Click **OK** or **Apply**.

Undefining Offline Permissions

You can reset previously set offline permissions to the unconfigured state. If offline permissions are undefined, regular permissions are applied to offline client computers.

To undefine offline permissions

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.

b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, select **Permissions**.

   When you select Permissions in the console tree, in the details pane you can view protocols for which you can set permissions. In the details pane you can also view the current state of offline permissions for each protocol in the Offline column.

4. In the details pane, right-click the protocol for which you want to undefine offline permissions, and then click **Undefine Offline**.

   You can undefine offline permissions set for several protocols at the same time. To do this, do the following:

   a) In the details pane, select several protocols by holding down the SHIFT key or the CTRL key while clicking them.
   b) Right-click the selection, and then click **Undefine Offline**.

   The offline state of the permissions changes to "Not Configured."

Removing Offline Permissions

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of higher-level offline permissions and enforce regular permissions on specific lower-level groups of client computers. To enforce regular permissions, you must remove offline permissions.

To remove offline permissions

1. If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, select **Permissions**.

   When you select Permissions in the console tree, in the details pane you can view protocols for which you can set permissions. In the details pane you can also view the current state of offline permissions for each protocol in the Offline column.

4. In the details pane, right-click the protocol for which you want to remove offline permissions, and then click **Remove Offline**.

You can remove offline permissions set for several protocols at the same time. To do this, do the following:

a) In the details pane, select several protocols by holding down the SHIFT key or the CTRL key while clicking them.
b) Right-click the selection and then click **Remove Offline**.

The offline state of the permissions changes to "Use Regular."

The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline Audit, Shadowing and Alerts for Protocols

For a detailed description of the Auditing & Shadowing feature for protocols, see "Managing Audit, Shadowing and Alerts for Protocols." For a detailed description of the Alerts feature, see "Alerts." For information about how to enable online (regular) alerts, see "Managing Audit, Shadowing and Alerts for Protocols." For information about how to enable offline alerts, see "Enabling Offline Alerts."

Offline audit, shadowing rules and alerts can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that audit, shadowing rules and alerts are not defined for a protocol. This is the default state.
Configured	Indicates that audit, shadowing rules and alerts are defined for a protocol.
No Audit	Indicates one of the following: • Audit rights are not set for all of the users and groups specified in audit and shadowing rules for a protocol. • All users and groups specified in audit and shadowing rules for a protocol. are removed. • The Everyone account has no Audit and Shadowing rights and is the only account specified in audit and shadowing rules for a protocol.
Use Regular	Indicates that the inheritance of offline audit and shadowing rules is blocked and regular audit and shadowing rules are enforced. Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of regular rules is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of regular rules lets you prevent offline rules inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of regular rules, see "Removing Offline Audit and Shadowing Rules."

Managing offline audit, shadowing rules and alerts involves the following tasks:

- Defining and editing offline audit and shadowing rules
- Enabling offline alerts
- Undefining offline audit and shadowing rules
- Removing offline audit and shadowing rules

Defining and Editing Offline Audit and Shadowing Rules

To define and edit offline audit and shadowing rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

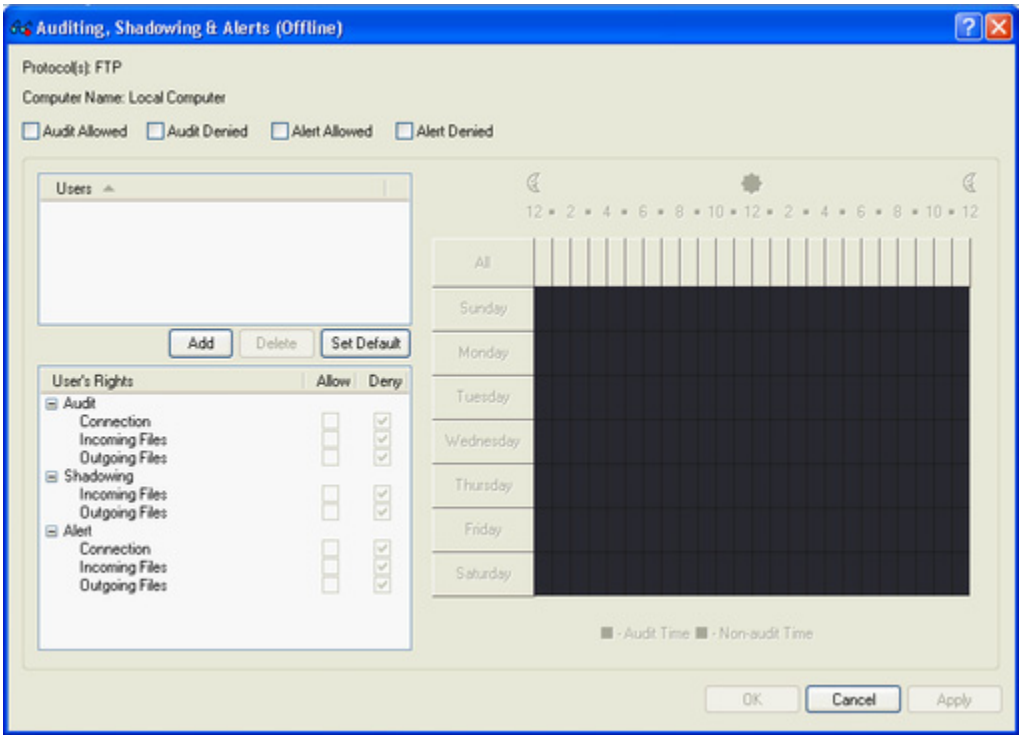
   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Auditing, Shadowing & Alerts**.

   When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view protocols for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each protocol in the Offline column.

4. In the details pane, do one of the following:
   - Right-click the protocol for which you want to define or edit rules, and then click **Set Offline Auditing, Shadowing & Alerts**.
     - OR -
   - Select the protocol for which you want to define or edit rules, and then click **Set Offline Auditing, Shadowing & Alerts** on the toolbar.

   The Auditing, Shadowing & Alerts (Offline) dialog box appears.



5. In the **Auditing, Shadowing & Alerts (Offline)** dialog box, do the following:

TO DO THIS	FOLLOW THESE STEPS
To define the default audit and shadowing rules	1. In the upper-left area of the dialog box, specify which events are written to the Audit Log. Select the **Audit Allowed** check box to audit successful attempts to gain access to a protocol. Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a protocol. 2. In the upper-left pane of the dialog box, under **Users**, click **Set Default**. *The default audit and shadowing rules apply to the Users and Everyone groups. For information about which Audit and Shadowing rights are set for these groups by default, see "Managing Audit, Shadowing and Alerts for Protocols."*
To define audit and shadowing rules for an additional user or group	1. In the upper-left area of the dialog box, specify which events are written to the Audit Log. Select the **Audit Allowed** check box to audit successful attempts to gain access to a protocol. Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a protocol. 2. In the upper-left pane of the dialog box, under **Users**, click **Add**. *The Select Users or Groups dialog box appears*. 3. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**. *The users and groups that you added are displayed under Users in the upper-left pane of the Auditing, Shadowing & Alerts (Offline) dialog box*. 4. In the upper-left pane of the **Auditing, Shadowing & Alerts**

TO DO THIS	FOLLOW THESE STEPS
	(Offline) dialog box, under **Users**, select the user or group. 5. *You can select multiple users and/ or groups by holding down the SHIFT key or the CTRL key while clicking them*. 6. In the lower-left pane of the **Auditing, Shadowing & Alerts (Offline)** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate audit and shadowing rights. *Audit and Shadowing rights determine which user actions on protocols are logged to the Audit and/or Shadow Log.* *In the right pane of the Auditing, Shadowing & Alerts (Offline) dialog box, you can specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on protocols will be logged to either the Audit or Shadow Log. Use the left mouse button to select days and hours when the selected user's actions on protocols will be logged. Use the right mouse button to mark days and hours when the selected user's actions on protocols will not be logged.*
To change audit and shadowing rules for an existing user or group	1. In the upper-left pane of the dialog box, under **Users**, select the user or group. 2. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate audit and shadowing rights.
To remove an existing user or group and rules	• In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key. *When you remove a user or group, any rules for* that *user or group will also be removed*.

6. Click **OK** or **Apply**.

Enabling Offline Alerts

Offline alerts for specific access-related events are enabled in the **Auditing, Shadowing & Alerts (Offline)** dialog box. Enabling offline alerts is similar to defining offline audit rules and includes the following basic steps:

- Specify which events will trigger alert notifications. You can enable notification of successful and/ or failed attempts to access a protocol. Select the **Alert Allowed** check box to enable notification of successful attempts to access a protocol. Select the **Alert Denied** check box to enable notification of failed attempts to access a protocol.
- Specify users and/or groups whose actions will trigger alert notifications. To do so, in the upper-left pane of the dialog box, under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.
- Specify which user's actions on protocols either will or will not trigger alert notifications. In the upper-left pane of the dialog box, under **Users**, select the user or group that you added. In the lower-left pane of the dialog box, under **User's**

Rights, select either **Allow** or **Deny** to directly allow or deny an alert right. Alert rights determine which user actions on protocols trigger alert notifications. Alert rights are identical to audit rights. The only difference is that when events matching specific criteria occur DeviceLock triggers alerts instead of logging these events in the Audit Log. For detailed information on Audit rights for protocols, see "Managing Audit, Shadowing and Alerts for Protocols."

- Specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on protocols either will or will not trigger alert notifications. To do so, in the right pane of the dialog box, use the left mouse button to select days and hours when the selected user's actions on protocols will trigger alert notifications. Use the right mouse button to mark days and hours when the selected user's actions on protocols will not trigger alert notifications.

Undefining Offline Audit and Shadowing Rules

You can return previously defined offline audit and shadowing rules to the unconfigured state. If offline rules are undefined, regular rules are applied to offline client computers.

To undefine offline audit and shadowing rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Auditing, Shadowing & Alerts**.

   When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view protocols for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each protocol in the Offline column.

4. In the details pane, right-click the protocol for which you want to undefine offline audit and shadowing rules, and then click **Undefine Offline**.

   You can undefine audit and shadowing rules defined for several protocols at the same time. To do this, do the following:
   a) In the details pane, select several protocols by holding down the SHIFT key or the CTRL key while clicking them.
   b) Right-click the selection, and then click **Undefine Offline**.

The offline state of the audit and shadowing rules changes to "Not Configured."

Removing Offline Audit and Shadowing Rules

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of higher-level offline audit and shadowing rules and enforce regular audit and shadowing rules on specific lower-level groups of client computers. To enforce regular audit and shadowing rules, you must remove offline audit and shadowing rules.

To remove offline audit and shadowing rules

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Auditing, Shadowing & Alerts**.

   When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view protocols for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each protocol in the Offline column.
4. In the details pane, right-click the protocol for which you want to remove offline audit and shadowing rules, and then click **Remove Offline**.

   You can remove audit and shadowing rules defined for several protocols at the same time. To do this, do the following:
   a) In the details pane, select several protocols by holding down the SHIFT key or the CTRL key while clicking them.
   b) Right-click the selection, and then click **Remove Offline**.

   The offline state of the audit and shadowing rules changes to "Use Regular."

   The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline Protocols White List

For a detailed description of the Protocols White List feature, see "Managing Protocols White List (Regular Profile)."

The offline Protocols White List can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that the white list is not defined. The following message is displayed: "Offline Protocols White List is not configured." This is the default state.
Configured	Indicates that the white list is defined.
Use Regular	Indicates that the inheritance of the offline white list is blocked and the regular white list is enforced. The following message is displayed: "Offline Protocols White List is configured to use Regular Protocols White List." Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of the regular white list is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of the regular white list lets you prevent the offline white list inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of the regular white list, see "Removing Offline Protocols White List."

Managing the offline Protocols White List involves the following tasks:

- Defining the offline Protocols White List
- Editing the offline Protocols White List
- Copying rules of the offline Protocols White List
- Exporting and importing the offline Protocols White List
- Deleting rules of the offline Protocols White List
- Undefining the offline Protocols White List
- Removing the offline Protocols White List

Defining Offline Protocols White List

To define the offline Protocols White List

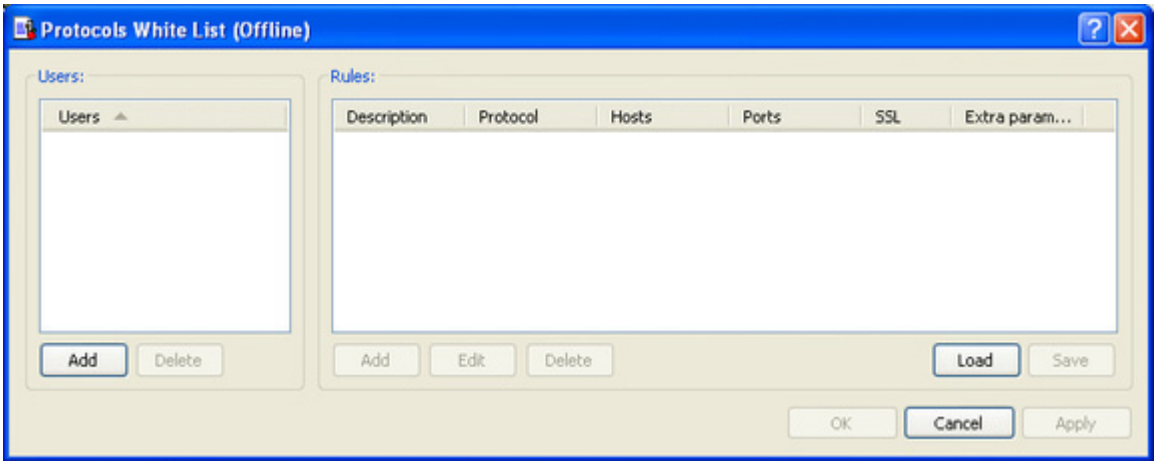
1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

- Right-click **White List**, and then click **Manage Offline**.
  - OR -
- Select **White List**, and then click **Manage Offline** on the toolbar.

The Protocols White List (Offline) dialog box appears.



4. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the Protocols White List, and then click **OK**.

   The users and groups that you added are displayed under Users in the left pane of the Protocols White List (Offline) dialog box.

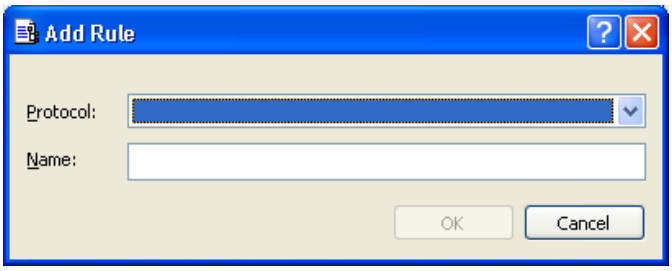
   To delete a user or group, in the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete**.

6. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the user or group.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

7. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, click **Add**.

   The Add Rule dialog box appears.



8. In the **Add Rule** dialog box, specify general and protocol-specific parameters for this rule. To specify general parameters, do the following:
    - To specify the protocol, in the **Protocol:** list, click the protocol of your choice.
    - To specify the rule name, in the **Name** box, type a name.

    To specify protocol-specific parameters, do the following:
    - To enable content inspection, click **Content Inspection**. For more information, see the description of the Content Inspection parameter earlier in this section.
    - To specify additional actions to be performed when this rule triggers, click **If this rule triggers**. For more information, see the description of the If this rule triggers parameter earlier in this section.
    - To specify the hosts, in the **Hosts:** box, type host names or IP addresses separated by a comma or semicolon. For more information on how to specify hosts, see the description of the Hosts parameter.
    - To specify the ports, in the **Ports:** box, type port numbers separated by a comma or semicolon. For more information on how to specify ports, see the description of the Ports parameter.
    - To specify the Web-based file storage, sharing and synchronization services, under **File Sharing Services:**, select the appropriate check boxes. For more information, see the description of the File Sharing Services parameter.
    - To configure the SSL options, under **SSL**, click any of the following: **Allowed** (allows SSL connections), **Denied** (disallows SSL connections), or **Required** (requires that all connections use SSL).
    - To specify the IM local sender ID(s), in the **Local sender ID(s):** box, type user identifiers separated by a comma or semicolon. For more information on how to specify user identifiers, see the description of the Local sender ID(s) parameter.
    - To specify the IM remote recipient ID(s), in the **Remote recipient ID(s):** box, type user identifiers separated by a comma or semicolon. For more information on how to specify user identifiers, see the description of the Remote recipient ID(s) parameter.
    - To specify the e-mail senders, in the **Local sender Email(s):** box, type sender addresses separated by a comma or semicolon. For more information on how to specify sender addresses, see the description of the Local sender Email(s): parameter.
    - To specify the e-mail recipients, in the **Remote recipient Email(s):** box, type recipient addresses separated by a comma or semicolon. For more information on how to specify recipient addresses, see the description of the Remote recipient Email(s): parameter.
    - To specify the social networking sites, under **Social Networks**:, select the appropriate check boxes. For more information, see the description of the Social Networks: parameter.
    - To specify the Web-based e-mail services, under **Web Mail Services**:, select the appropriate check boxes. For more information, see the description of the Web Mail Services: parameter.

9. Click **OK**.

    The rule you created is displayed under Rules in the right pane of the Protocols White List (Offline) dialog box.

10. Click **OK** or **Apply**.

    The users or groups to which the white list rule applies are displayed under White List in the console tree.

    When you select a user or group to which a white list rule applies in the console tree, in the details pane you can view detailed information regarding this rule. This information includes the following:

    - **Protocol** The protocol the rule applies to.
    - **Name** The name of the rule.
    - **Hosts** Shows the allowed hosts for this rule.
    - **Ports** Shows the allowed ports for this rule.
    - **SSL** Shows the selected SSL option. Possible values: **Allowed** (allows SSL connections), **Denied** (disallows SSL connections), and **Required** (requires that all connections use SSL).
    - **Content Inspection** Shows whether the content inspection is enabled or not.
    - **Extra parameters** Shows additional protocol-specific parameters specified for the rule. These parameters include: **From** (shows allowed sender identifiers for instant messaging and e-mail sender addresses for Webmail) and **To** (shows allowed recipient identifiers for instant messaging and e-mail recipient addresses for Webmail).
    - **Profile** Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to computers that are working offline.

      You can define different online vs. offline Protocols White Lists for the same user or sets of users. For information about how to define the online Protocols White List, see "Managing Protocols White List."

Editing Offline Protocols White List

You can modify parameter values specified for an offline white list rule any time you want.

To edit an offline white list rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **White List**, click **Manage Offline**, and then do the following:

a) In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the user or group for which you want to edit the rule.
By selecting users or groups, you can view the white list rules applied to them under Rules in the right pane of the dialog box.
b) In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.
- OR -
Right-click the rule, and then click **Edit**.

- OR -

Under **Protocols**, expand **White List**, and then do the following:

a) Under **White List**, select the user or group for which you want to edit the rule.
By selecting users or groups, you can view the white list rules applied to them in the details pane.
b) In the details pane, right-click the rule you want to edit, and then click **Edit**.
- OR -
In the details pane, double-click the rule you want to edit.

The Edit Rule dialog box appears.

4. In the **Edit Rule** dialog box, modify the rule parameters as required to meet your needs.
5. Click **OK** to apply the changes.

Copying Rules of Offline Protocols White List

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing rules of the offline Protocols White List.

To copy an offline white list rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **White List**, and then click **Manage Offline**.
     - OR -
   - Select **White List**, and then click **Manage Offline** on the toolbar.

The Protocols White List (Offline) dialog box appears.

4. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.

   By selecting users or groups, you can view the white list rules applied to them under Rules in the right pane of the dialog box.

5. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

   The rule you cut or copy is automatically copied to the Clipboard.

   You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.

6. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the left pane of the Protocols White List (Offline) dialog box.

8. In the left pane of the **Protocols White List (Offline)**dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

9. In the right pane of the **Protocols White List (Offline)** dialog box, right-click in the **Rules** pane and then click **Paste**.

   The copied rule is displayed under Rules in the right pane of the Protocols White List dialog box.

10. Click **OK** or **Apply** to apply the copied rule.

Exporting and Importing Offline Protocols White List

You can export all your current rules of the offline Protocols White List to a .pwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

To export the offline Protocols White List

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

- Right-click **White List**, and then click **Save Offline**.
  - OR -
- Select **White List**, and then click **Save Offline** on the toolbar.
  - OR -
- Expand **White List**, right-click any user or group specified in the white list, and then click **Save Offline**.
  - OR -
- Expand **White List**, select any user or group specified in the white list. In the details pane, right-click the white list rule, and then click **Save**.
  - OR –
- Expand **White List**, select any user or group specified in the white list, and then click **Save Offline** on the toolbar.
  - OR -
- Right-click **White List**, and then click **Manage Offline**. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, click **Save**.

The Save As dialog box appears.

4. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the .pwl file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.

When you export the offline Protocols White List, it is saved in a file with a .pwl extension.

To import the offline Protocols White List

1. If you use DeviceLock Management Console, do the following:

a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

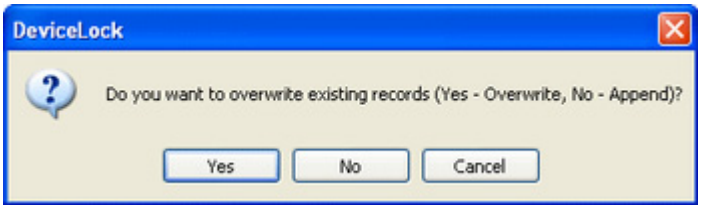
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

- Right-click **White List**, and then click **Load Offline**.
  - OR -
- Select **White List**, and then click **Load Offline** on the toolbar.
  - OR -
- Expand **White List**, right-click any user or group specified in the white list, and then click **Load Offline**.
  - OR -
- Expand **White List**, select any user or group specified in the white list. In the details pane, right-click the white list rule, and then click **Load**.
  - OR –
- Expand **White List**, select any user or group specified in the white list, and then click **Load Offline** on the toolbar.
  - OR-
- Right-click **White List**, and then click **Manage Offline**. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules,** click **Load**.

The Open dialog box appears.

4. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
5. In the folder list, locate and open the folder that contains the file.
6. Click the file, and then click **Open.**

   If the offline Protocols White List is already defined and you choose to import a new offline white list, the following message box is displayed.



   In the message box, click **Yes** to overwrite the existing offline white list. Click **No** to append a new offline white list to the existing offline white list.

Deleting Rules of Offline Protocols White List

You can delete individual rules of the offline Protocols White List when they are no longer required.

To delete an offline white list rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

- Expand **White List**, right-click the user or group to which the rule is applied, and then click **Delete user**.
  When you delete a user or group, the rule associated with this user or group is automatically deleted.
  - OR -
- Expand **White List**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.
  - OR -
- Right-click **White List**, and then click **Manage Offline**. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the user or group to which the rule is applied. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.

Undefining Offline Protocols White List

You can return the previously defined offline white list to the unconfigured state. If the offline white list is undefined, the regular white list is applied to offline client computers.

To undefine the offline Protocols White List

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, right-click **White List**, and then click **Undefine Offline**.

   The offline state of the white list changes to "Not Configured."

   When you select **White List** in the console tree, in the details pane the following message is displayed: "Offline Protocols White List is not configured."

Removing Offline Protocols White List

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of the higher-level offline white list and enforce the regular white list on specific lower-level groups of client computers. To enforce the regular Protocols White List, you must remove the offline Protocols White List.

To remove the offline Protocols White List

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **White List**, and then click **Remove Offline**.

   The offline state of the white list changes to "Use Regular."

   When you select **White List** in the console tree, in the details pane the following message is displayed: "Offline Protocols White List is configured to use Regular Protocols White List."

   The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline IP Firewall

For a detailed description of the Basic IP Firewall feature, see "Managing Basic IP Firewall (Regular Profile)."

The offline IP Firewall can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that the IP Firewall is not configured. The following message is displayed: "Offline Basic IP Firewall is not configured." This is the default state.
Configured	Indicates that the IP Firewall is configured.
Use Regular	Indicates that the inheritance of the offline IP Firewall is blocked and the regular IP Firewall is enforced. The following message is displayed: "Offline Basic IP Firewall is configured to use Regular Basic IP Firewall." Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of the regular IP Firewall is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of the regular IP Firewall lets you prevent the offline IP Firewall inherited from a higher level from being applied to a specific

STATE	DESCRIPTION
	group of client computers at a lower level. For more information on the enforcement of the regular IP Firewall, see "Removing Offline Firewall Rules."

Managing offline firewall rules involves the following tasks:

- Defining offline firewall rules
- Editing offline firewall rules
- Copying offline firewall rules
- Exporting and importing offline firewall rules
- Deleting offline firewall rules
- Undefining offline firewall rules
- Removing offline firewall rules

Defining Offline Firewall Rules

You can enable offline alerts that are sent when a specific offline firewall rule fires. Such alerts are enabled at the time you define an offline firewall rule.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific firewall rule, you must configure alert settings in **Service Options**.

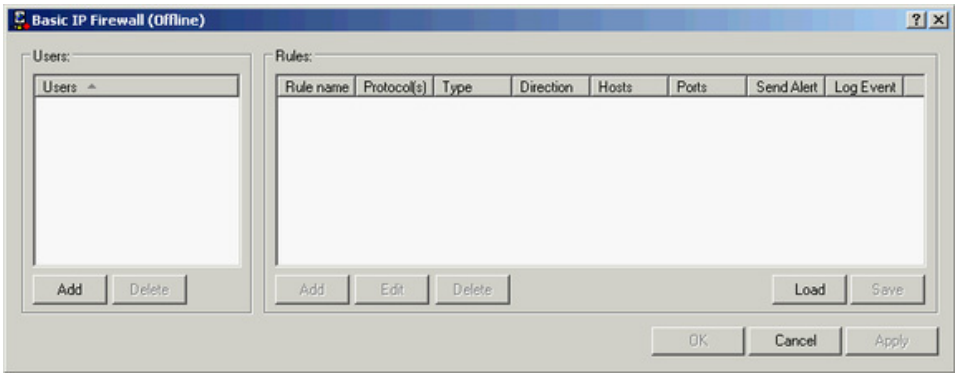
To define an offline firewall rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock.**
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Basic IP Firewall**, and then click **Manage Offline**.
     - OR -
   - Select **Basic IP Firewall**, and then click **Manage Offline** on the toolbar.

The Basic IP Firewall (Offline) dialog box appears.



4. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the firewall rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the left pane of the Basic IP Firewall (Offline) dialog box.

   To delete a user or group, in the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete**.

6. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the user or group.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

7. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, click **Add**.

   The Add Rule dialog box appears.

8. In the **Add Rule** dialog box, specify the firewall rule parameters:

   - To specify the rule name, in the **Name** box, type a name.
   - To specify the protocol, under **Protocol**, select the check box next to the protocol of your choice.
   - To specify what actions the firewall takes for all connections that match the rule's criteria, under **Type**, click either of the following options: **Allow** or **Deny**.
   - To specify the direction of traffic to which the rule applies, under **Direction**, select the appropriate check box.
   - To specify additional actions to be performed when the rule triggers, under **If this rule triggers**, select the appropriate check box.
   - To specify the remote hosts to which the rule applies, in the **Hosts:** box, type host names or IP addresses separated by a comma or semicolon.
   - To specify the ports on remote hosts to which the rule applies, in **the Ports:** box, type port numbers separated by a comma or semicolon.

   For more information, see the description of the firewall rule parameters.

9. Click **OK**.

   The rule you created is displayed under Rules in the right pane of the Basic IP Firewall (Offline) dialog box.

10. Click **OK** or **Apply**.

    The users or groups to which the firewall rule applies are displayed under Basic IP Firewall in the console tree.

    When you select a user or group to which a firewall rule applies in the console tree, in the details pane you can view detailed information regarding this rule. This information includes the following:

    - **Name** The name of the rule.
    - **Protocol(s)** The protocol(s) to which the rule applies: **TCP** and/or **UDP**.
    - **Type** The action the firewall takes for all connections that match the rule's criteria. Possible actions: **Allow** (allows the connection) and **Deny** (blocks the connection).
    - **Direction** The direction of traffic to which the rule applies: **Incoming** and/or **Outgoing**.
    - **Hosts** Shows the specified hosts for this rule.
    - **Ports** Shows the specified ports for this rule.
    - **Send Alert** Shows whether alerts are enabled or disabled for this rule.
    - **Log Event** Shows whether audit logging of events associated with this rule is enabled or disabled.
    - **Profile** Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to client computers that are working offline.

      You can define different online vs. offline firewall rules for the same user or sets of users. For information about how to define online firewall rules, see "Managing Basic IP Firewall."

Editing Offline Firewall Rules

You can modify parameter values specified for an offline firewall rule any time you want.

To edit an offline firewall rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined offline DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.

b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, right-click **Basic IP Firewall**, click **Manage Offline**, and then do the following:

   a) In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the user or group for which you want to edit the rule.

   By selecting users or groups, you can view the firewall rules applied to them under Rules in the right pane of the dialog box.

   b) In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.

   - OR -

   Right-click the rule, and then click **Edit**.

   - OR -

   Under **Protocols**, expand **Basic IP Firewall**, and then do the following:

   a) Under **Basic IP Firewall**, select the user or group for which you want to edit the rule.

   By selecting users or groups, you can view the firewall rules applied to them in the details pane.

   b) In the details pane, right-click the rule you want to edit, and then click **Edit**.

   - OR -

   In the details pane, double-click the rule you want to edit.

   The Edit Rule dialog box appears.

4. In the **Edit Rule** dialog box, modify the rule parameters as required to meet your needs.
5. Click **OK** to apply the changes.

Copying Offline Firewall Rules

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing offline firewall rules.

To copy an offline firewall rule

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.

   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.

   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined offline DeviceLock policies.

   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Basic IP Firewall**, and then click **Manage Offline**.
     - OR -
   - Select **Basic IP Firewall**, and then click **Manage Offline** on the toolbar.

   The Basic IP Firewall (Offline) dialog box appears.
4. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.

   By selecting users or groups, you can view the firewall rules applied to them under Rules in the right pane of the dialog box.
5. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

   The rule you cut or copy is automatically copied to the Clipboard.

   You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.

   You can copy and then paste several rules at the same time. Hold down the SHIFT key or the CTRL key while you click each rule, right-click one of them, and then click **Copy**.
6. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.
7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the left pane of the Basic IP Firewall (Offline) dialog box.
8. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.
9. In the right pane of the **Basic IP Firewall (Offline)** dialog box, right-click in the **Rules** pane and then click **Paste**.

   The copied rule is displayed under Rules in the right pane of the Basic IP Firewall (Offline) dialog box.
10. Click **OK** or **Apply** to apply the copied rule.

Exporting and Importing Offline Firewall Rules

You can export all your current offline firewall rules to an .ipp file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

To export offline firewall rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined offline DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Basic IP Firewall**, and then click **Save Offline**.
     - OR -
   - Select **Basic IP Firewall**, and then click **Save Offline** on the toolbar.
     - OR -
   - Expand **Basic IP Firewall**, right-click any user or group specified in the firewall rule, and then click **Save Offline**.
     - OR -
   - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule. In the details pane, right-click the firewall rule, and then click **Save**.
     - OR –
   - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule, and then click **Save Offline** on the toolbar.
     - OR -
   - Right-click **Basic IP Firewall**, and then click **Manage Offline**. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, click **Save**.

   The Save As dialog box appears.
4. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the .ipp file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.

   When you export offline firewall rules, they are saved in a file with an .ipp extension.

To import offline firewall rules

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

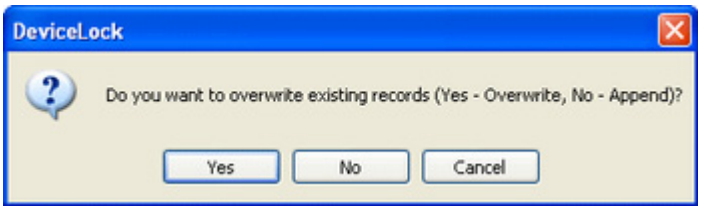
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

   - Right-click **Basic IP Firewall**, and then click **Load Offline**.
     - OR -
   - Select **Basic IP Firewall**, and then click **Load Offline** on the toolbar.
     - OR -
   - Expand **Basic IP Firewall**, right-click any user or group specified in the firewall rule, and then click **Load Offline**.
     - OR -
   - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule. In the details pane, right-click the firewall rule, and then click **Load**.
     - OR -
   - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule, and then click **Load Offline** on the toolbar.
     - OR -
   - Right-click **Basic IP Firewall**, and then click **Manage Offline**. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, click **Load**.

   The Open dialog box appears.

4. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
5. In the folder list, locate and open the folder that contains the file.
6. Click the file, and then click **Open**.

   If offline firewall rules are already defined and you choose to import new offline firewall rules, the following message box is displayed.



In the message box, click **Yes** to overwrite the existing offline firewall rules. Click **No** to append new offline firewall rules to the existing offline firewall rules.

Deleting Offline Firewall Rules

You can delete individual offline firewall rules when they are no longer required.

To delete an offline firewall rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined offline DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Expand **Basic IP Firewall**, right-click the user or group to which the rule is applied, and then click **Delete user**.
     When you delete a user or group, the rule associated with this user or group is automatically deleted.
     - OR -
   - Expand **Basic IP Firewall**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.
     - OR -
   - Right-click **Basic IP Firewall**, and then click **Manage Offline**. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the user or group to which the rule is applied. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.

Undefining Offline Firewall Rules

You can return the previously defined offline firewall rules to the unconfigured state. If offline firewall rules are undefined, regular firewall rules are applied to offline client computers.

To undefine offline firewall rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined offline DeviceLock policies.
   c) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Undefine Offline**.

   The offline state of the IP Firewall changes to "Not Configured."

   When you select **Basic IP Firewall** in the console tree, in the details pane the following message is displayed: "Offline Basic IP Firewall is not configured."

Removing Offline Firewall Rules

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of higher-level offline firewall rules and enforce regular firewall rules on specific lower-level groups of client computers. To enforce regular firewall rules, you must remove offline firewall rules.

To remove offline firewall rules

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Remove Offline**.

The offline state of the IP Firewall changes to "Use Regular."

When you select **Basic IP Firewall** in the console tree, in the details pane the following message is displayed: "Offline Basic IP Firewall is configured to use Regular Basic IP Firewall."

The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline Content-Aware Rules for Protocols

For a detailed description of the Content-Aware Rules feature for protocols, see "Content-Aware Rules for Protocols (Regular Profile)."

The offline Content-Aware Rules can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that Content-Aware Rules are not defined. The following message is displayed: "Offline Content-Aware Rules are not configured." This is the default state.
Configured	Indicates that Content-Aware Rules are defined.
Use Regular	Indicates that the inheritance of offline Content-Aware Rules is blocked and regular Content-Aware Rules are enforced. Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of regular Content-Aware Rules is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of regular Content-Aware Rules lets you prevent offline Content-Aware Rules inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of regular Content-Aware Rules, see "Removing Offline Content-Aware Rules."

Managing offline Content-Aware Rules involves the following tasks:

- Defining offline Content-Aware Rules
- Editing offline Content-Aware Rules
- Copying offline Content-Aware Rules
- Exporting and importing offline Content-Aware Rules
- Deleting offline Content-Aware Rules
- Undefining offline Content-Aware Rules
- Removing offline Content-Aware Rules

Defining Offline Content-Aware Rules

Content-Aware Rules are created based on either the built-in or custom content groups. For detailed information on these groups, see "Configuring Content Detection Settings."

You can enable offline alerts that are sent when a specific offline Content-Aware Rule fires. Such alerts are enabled at the time you define an offline Content-Aware Rule.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific Content-Aware Rule, you must configure alert settings in **Service Options**.

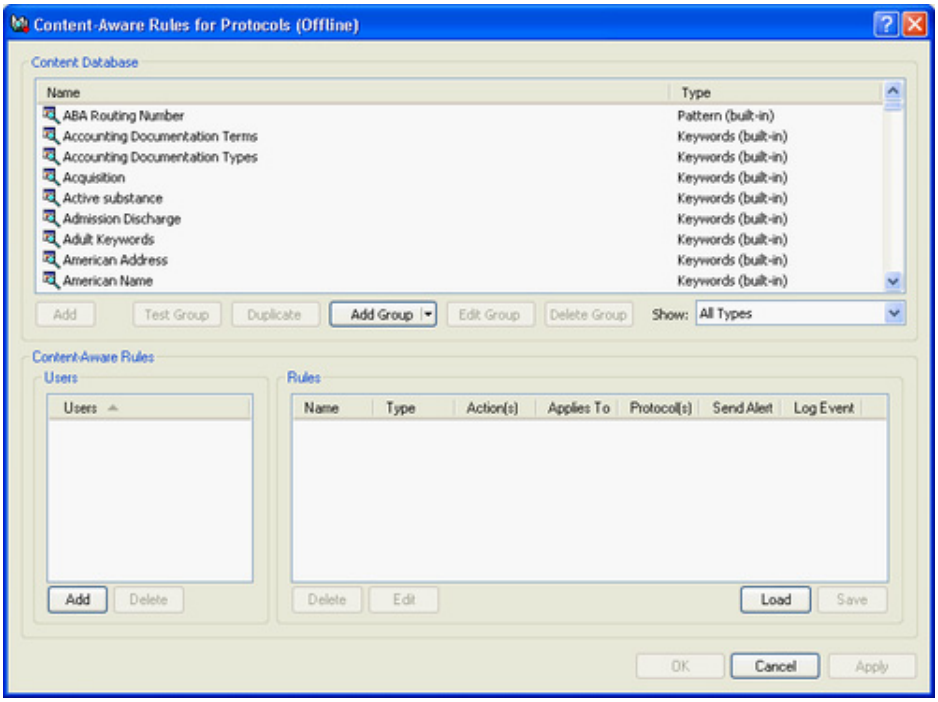
To define an offline Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage Offline**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage Offline** on the toolbar.

   The Content-Aware Rules for Protocols (Offline) dialog box appears.



4. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Protocols (Offline) dialog box.

   To delete a user or group, in the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

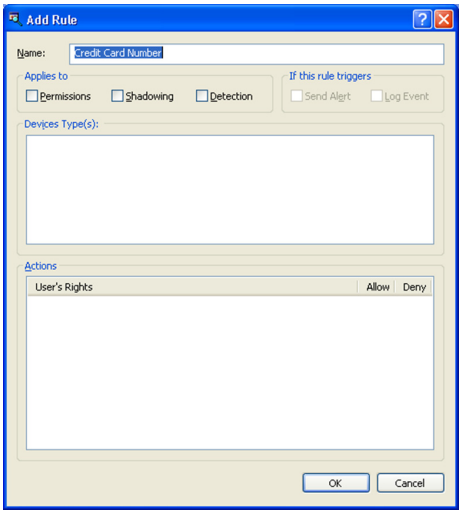
6. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the users or groups for which you want to define the rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

7. In the upper pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Content Database**, select the desired content group, and then click **Add**.

   Note: You can specify only one content group for a Content-Aware Rule.

   The Add Rule dialog box appears.



8. In the **Add Rule** dialog box, in the **Name** box, type the name of the Content-Aware Rule.

   By default, the Content-Aware Rule has the same name as the specified content group but you can enter a different name.

9. Under **Applies to**, specify the type of operation associated with the rule. The available options are:

   - **Permissions**: Specifies that the rule will apply to access control operations.
   - **Shadowing**: Specifies that the rule will apply to shadow copy operations.

- **Detection**: Specifies that the rule will apply to detection operations.
- **Permissions**, **Shadowing**: Specifies that the rule will apply to both access control and shadow copy operations.
- **Permissions, Detection**: Specifies that the rule will apply to both access control and detection operations.
- **Shadowing, Detection**: Specifies that the rule will apply to both shadow copy and detection operations.
- **Permissions, Shadowing, Detection**: Specifies that the rule will apply to all available operations: access control, shadow copy, and detection.

10. Under **If this rule triggers**, specify the following additional actions to be performed when the rule triggers:

    - **Send Alert**: Specifies that an alert is sent whenever the rule triggers.
    - **Log Event**: Specifies that an event is logged in the Audit Log whenever the rule triggers.

11. Under **Protocol(s)**, select the appropriate protocol(s) you would like this rule to be applied to.

    Content-Aware Rules can be applied to the following protocols: File Sharing, FTP, HTTP, IBM Notes, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, MAPI, SMB, SMTP, Skype, Social Networks, Web Mail, Windows Messenger, and Yahoo Messenger.

    Under Action(s), if you multi-select protocols that have different combinations of configurable access rights, the dialog box will display the superset of access rights for the selection list: those that are common to all selected protocols, and those that do not necessarily apply to all protocols. As would be expected, if a particular access right that is displayed is not common to one or more particular selected protocols, it's setting will not/cannot be applied to those protocols and will only apply to protocols where the setting is supported.

12. Under **Action(s)**, specify which user actions are allowed or disallowed on protocols, which user actions are logged to the Shadow Log, and which user actions are detected.

    If the rule applies to shadow copy operations combined with other operations, the Read user right becomes unavailable. If the rule applies to detection operations combined with other operations, only Allow action becomes available. For detailed information on user rights and actions that can be specified in Content-Aware Rules, see "Content-Aware Rules for Access Control Operations", "Content-Aware Rules for Shadow Copy Operations" and "Content-Aware Rules for Detection Operations".

13. Click **OK**.

    The rule you created is displayed under Rules in the lower-right pane of the Content-Aware Rules for Protocols (Offline) dialog box.

14. Click **OK** or **Apply** to apply the rule.

    The users or groups to which the Content-Aware Rule applies are displayed under Content-Aware Rules in the console tree. When you select a user or group to which a Content-Aware Rule applies in the console tree, in the details pane you can view detailed information regarding this rule. This information includes the following:

- **Name** The name of the rule. By default, the rule has the same name as the specified content group.
- **Type** The type of the content analysis. Possible values: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties**, **Complex** and **Oracle IRM**. **File Type Detection** indicates that recognition and identification of files is based on their characteristic signatures. **Keywords** indicates that recognition and identification of data/files is based on the specified keywords or phrases. **Pattern** indicates that recognition and identification of data/files is based on the specified patterns of text described by Perl regular expressions. **Document Properties** indicates that recognition and identification of files is based on their properties. **Complex** indicates that recognition and identification of data/files is based on the specified content described by a Boolean expression. **Oracle IRM** indicates that recognition and identification of files is based on their IRM contexts.
- **Action(s)** Shows which user actions are allowed or disallowed on protocols and which user actions are logged to the Shadow Log.
- **Applies To** Possible values: **Permissions**, **Shadowing**, **Detection**, **Permissions+Shadowing, Permissions+Detection, Shadowing+Detection, Permissions+Shadowing+Detection**. **Permissions** indicates that the rule applies to access control operations. **Shadowing** indicates that the rule applies to shadow copy operations. **Detection** indicates that the rule applies to detection operations. **Permissions+Shadowing** indicates that the rule applies to both access control and shadow copy operations. **Permissions+Detection** indicates that the rule applies to both access control and detection operations. **Shadowing+Detection** indicates that the rule applies to both shadow copy and detection operations. **Permissions+Shadowing+Detection** indicates that the rule applies to all available operations: access control, shadow copy, and detection.
- **Protocol(s)** The protocol(s) to which the rule applies.
- **Send Alert** Shows whether alerts are enabled or disabled for this rule.
- **Log Event** Shows whether audit logging of events associated with this rule is enabled or disabled.
- **Profile** Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to computers that are working offline.

  You can define different online vs. offline Content-Aware Rules for the same user or sets of users. For information about how to define online Content-Aware Rules for protocols, see "Managing Content-Aware Rules."

Editing Offline Content-Aware Rules

You can modify the Content-Aware Rule properties such as **Name**, **Applies To**, **If this rule triggers**, **Protocol(s)**, **Actions**.

To edit an offline Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, right-click **Content-Aware Rules**, click **Manage Offline**, and then do the following:

   a) In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the user or group for which you want to edit the rule.
   By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.

   b) In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.

   - OR -

   Under **Protocols**, expand **Content-Aware Rules**, and then do the following:

   a) Under **Content-Aware Rules**, select the user or group for which you want to edit the rule.
   By selecting users or groups, you can view the Content-Aware Rules applied to them in the details pane.

   b) In the details pane, right-click the rule you want to edit, and then click **Edit**.
   - OR -
   In the details pane, double-click the rule you want to edit.

   The Edit Rule dialog box appears.

4. In the **Edit Rule** dialog box, modify the rule properties as required to meet your needs.
5. Click **OK** to apply the changes.

Copying Offline Content-Aware Rules

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing offline Content-Aware Rules.

To copy an offline Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Manage Offline**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Manage Offline** on the toolbar.

   The Content-Aware Rules for Protocols (Offline) dialog box appears.

4. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.

   By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.

5. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

   The rule you cut or copy is automatically copied to the Clipboard.

   You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.

   To perform a drag-and-drop operation, select the rule and move it to the user or group to which you want to apply the copied rule.

6. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, click **Add**.

   The Select Users or Groups dialog box appears.

7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

   The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Protocols (Offline) dialog box.

8. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.

   You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

9. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, right-click in the **Rules** pane and then click **Paste**.

   The copied rule is displayed under Rules in the lower-right pane of the Content-Aware Rules for Protocols (Offline) dialog box.

10. Click **OK** or **Apply** to apply the copied rule.

Exporting and Importing Offline Content-Aware Rules

You can export all your current offline Content-Aware Rules to a .cwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

To export offline Content-Aware Rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Right-click **Content-Aware Rules**, and then click **Save Offline**.
     - OR -
   - Select **Content-Aware Rules**, and then click **Save Offline** on the toolbar.
     - OR -
   - Expand **Content-Aware Rules**, right-click any user or group to which the rule is applied, and then click **Save Offline**.
     - OR -
   - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Save**.
     - OR -
   - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Save Offline** on the toolbar.
     - OR -
   - Right-click **Content-Aware Rule**s, and then click **Manage Offline**. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Rules**, click **Save**.

   The Save As dialog box appears.

4. In the **Save As** dialog box, in the **Save in** box, browse to the location where you want to save the .cwl file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.

   When you export rules, they are saved in a file with a .cwl extension.

To import offline Content-Aware Rules

1. If you use DeviceLock Management Console, do the following:

   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:

   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**., do one of the following:

   - Right-click **Content-Aware Rules**, and then click **Load Offline**.

     - OR -
   - Select **Content-Aware Rules**, and then click **Load Offline** on the toolbar.

     - OR -
   - Expand **Content-Aware Rules**, right-click any user or group to which the rule is applied, and then click **Load Offline**.

     - OR -
   - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Load**.

     - OR -
   - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Load Offline** on the toolbar.

     - OR -
   - Right-click **Content-Aware Rules**, and then click **Manage Offline**. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Rules**, click **Load**.

   The Open dialog box appears.

4. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
5. In the folder list, locate and open the folder that contains the file.

6. Click the file, and then click **Open**.

   You can import only one .cwl file at a time.

Deleting Offline Content-Aware Rules

You can delete individual offline Content-Aware Rules when they are no longer required.

To delete an offline Content-Aware Rule

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
   - Expand **Content-Aware Rules**, right-click the user or group to which the rule is applied, and then click **Delete user**.
     When you delete a user or group, the rule associated with this user or group is automatically deleted.

     - OR -
   - Expand **Content-Aware Rules**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.
     - OR -
   - Right-click **Content-Aware Rules**, and then click **Manage Offline**. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the user or group to which the rule is applied. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Rules**, select the rule, and then click **Delete**.
     You can select multiple rules that you want to delete by holding down the SHIFT key or the CTRL key while clicking them.

Undefining Offline Content-Aware Rules

You can return the previously defined offline Content-Aware Rules to the unconfigured state. If offline rules are undefined, regular rules are applied to offline client computers.

To undefine offline Content-Aware Rules

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Content-Aware Rules**, and then click **Undefine Offline**.

   The offline state of Content-Aware Rules changes to "Not Configured."

   When you select **Content-Aware Rules** in the console tree, in the details pane the following message is displayed: "Offline Content-Aware Rules are not configured."

Removing Offline Content-Aware Rules

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of higher-level offline Content-Aware Rules and enforce regular Content-Aware Rules on specific lower-level groups of client computers. To enforce regular Content-Aware Rules, you must remove offline Content-Aware Rules.

To remove offline Content-Aware Rules

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Content-Aware Rules**, and then click **Remove Offline**.

   The offline state of Content-Aware Rules changes to "Use Regular."

   When you select **Content-Aware Rules** in the console tree, in the details pane the following message is displayed: "Offline Content-Aware Rules are configured to use Regular Content-Aware Rules."

The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Managing Offline Security Settings for Protocols

For a detailed description of the Security Settings feature for protocols, see "Managing Security Settings for Protocols."

Offline Security Settings can have one of the following states:

STATE	DESCRIPTION
Not Configured	Indicates that Security Settings are not defined for protocols. This is the default state.
Enabled	Indicates that Security Settings are enabled for protocols.
Disabled	Indicates that Security Settings are disabled for protocols.
Use Regular	Indicates that the inheritance of offline Security Settings is blocked and regular Security Settings are enforced. Offline DeviceLock settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of regular Security Settings is useful if you use Group Policy or DeviceLock Service Settings files (.dls) to deploy DeviceLock policies throughout your network. The enforcement of regular Security Settings lets you prevent offline Security Settings inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of regular Security Settings, see "Removing Offline Security Settings."

Managing offline Security Settings involves the following tasks:

- Defining and changing offline Security Settings
- Undefining offline Security Settings
- Removing offline Security Settings

Defining and Changing Offline Security Settings

To define and change offline Security Settings

1. If you use DeviceLock Management Console, do the following:
   a) Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

- Select **Security Settings**. In the details pane, right-click the **Security Setting,** and then click **Enable Offline** or **Disable Offline**.
  When you select Security Settings in the console tree, they are displayed in the details pane.

  - OR-
- Right-click **Security Settings**, and then click **Manage Offline**. In the **Security Settings (Offline)** dialog box that opens, select or clear the appropriate check box, and then click **OK**.
  To open the Security Settings (Offline) dialog box, you can also select Security Settings, and then click Manage Offline *on the toolbar.*

Note: All check boxes in the **Security Settings (Offline)** dialog box have three states: selected, cleared, and indeterminate that correspond to the Enabled, Disabled, and Not Configured states of Security Settings.

The Security Setting changes its offline state from "Not Configured" to "Enabled" or "Disabled."

Undefining Offline Security Settings

You can return the previously defined offline Security Settings to the unconfigured state. If offline Security Settings are undefined, regular Security Settings are applied to offline client computers.

To undefine offline Security Settings

1. If you use DeviceLock Service Settings Editor, do the following:

a) Open DeviceLock Service Settings Editor.
b) In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the XML file with defined offline DeviceLock policies.
c) In the console tree, expand **DeviceLock Service**.

If you use DeviceLock Group Policy Manager, do the following:

a) Open Group Policy Object Editor.
b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:

- Select **Security Settings**. In the details pane, right-click the Security Setting, and then click **Undefine Offline**.
  When you select Security Settings in the console tree, they are displayed in the details pane.

- OR –

- Right-click **Security Settings**, and then click **Manage Offline**. In the **Security Settings (Offline)** dialog box that opens, return the appropriate check box to the indeterminate state, and then click **OK**.

  To open the Security Settings (Offline) dialog box, you can also select Security Settings, and then click Manage Offline *on the toolbar.*

Note: All check boxes in the **Security Settings (Offline)** dialog box have three states: selected, cleared, and indeterminate that correspond to the Enabled, Disabled, and Not Configured states of Security Settings.

The Security Setting changes its offline state to "Not Configured."

Removing Offline Security Settings

If you deploy DeviceLock policies using Group Policy or DeviceLock Service Settings files (.dls), DeviceLock provides you with the ability to block the inheritance of higher-level offline Security Settings and enforce regular Security Settings on specific lower-level groups of client computers. To enforce regular Security Settings, you must remove offline Security Settings.

To remove offline Security Settings

1. If you use DeviceLock Service Settings Editor, do the following:
   a) Open DeviceLock Service Settings Editor.
   b) In the console tree, expand **DeviceLock Service**.

   If you use DeviceLock Group Policy Manager, do the following:
   a) Open Group Policy Object Editor.
   b) In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Security Settings.**

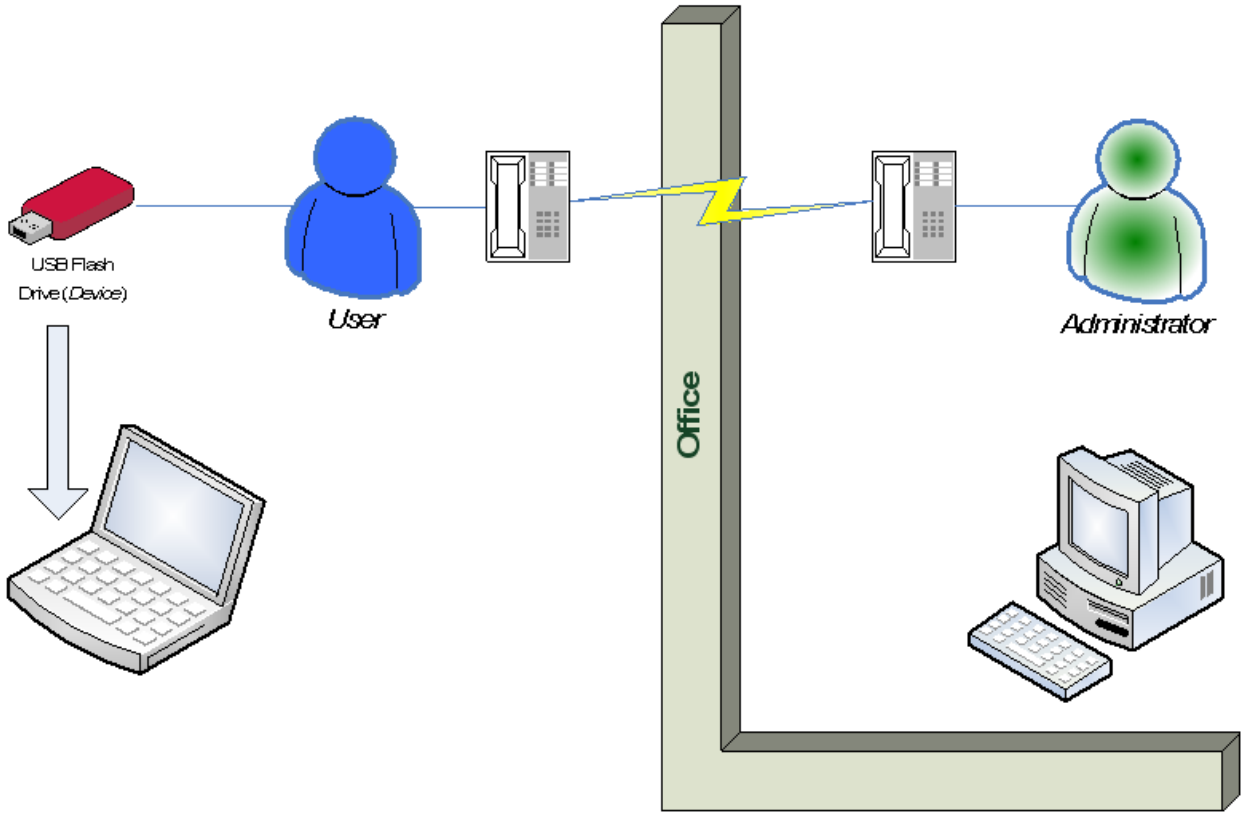
   When you select Security Settings in the console tree, they are displayed in the details pane.
4. In the details pane, right-click the Security Setting, and then click **Remove Offline**.

   The Security Setting changes its offline state to "Use Regular."

   The "Use Regular" state of DeviceLock settings is displayed as "Not Configured" in DeviceLock Management Console.

Temporary White List

The DeviceLock Temporary White List function enables the granting of temporary access to USB devices when there is no network connection. Administrators provide users with special access codes over the phone that temporarily unlock access to requested devices. The following diagram illustrates the process of granting temporary access to USB devices.



A Temporary White List works like a device white list, with the distinction that a network connection is not required to add devices and grant access to them.

Note: Using Temporary White List it is possible to grant access to USB devices that were blocked on both levels: the USB port level and the type level. If some white listed device (for example, USB Flash Drive) belongs to both levels: USB and type (Removable), the permissions (if any) for the type level are ignored as well as for the USB level.

Creating and activating a Temporary White List is a matter of following these step-by-step instructions:

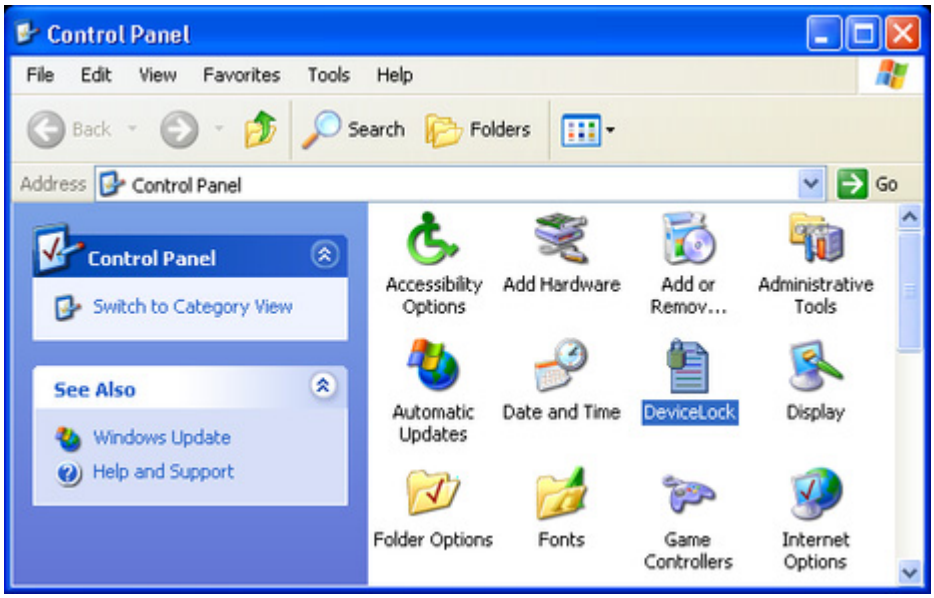
1. The administrator generates a cryptographic certificate (DeviceLock Certificate) using the Certificate Generation Tool. A DeviceLock Certificate consists of two keys: private and public.
2. The administrator deploys the DeviceLock Certificate (the public key) to a user's computer. This enables the Temporary White List on the user's computer.

3. When a user needs to access some USB device, he/she runs the Temporary White List Authorization Tool from the Windows Control Panel. Then the user selects the particular device from a list and a textual-numeric code (**Device Code**) is generated. The user can then provide this code to the DeviceLock Administrator over the phone or via an Internet chat session.
4. The administrator then runs the DeviceLock Signing Tool, loads the corresponding DeviceLock Certificate (the private key), enters the **Device Code**, selects an appropriate temporary access period (5, 15, etc. minutes, until the device is unplugged or until the user is logged off), generates an **Unlock Code**, and relays this **Unlock Code** to the user.
5. Upon receipt of the **Unlock Code**, the user enters it into Temporary White List Authorization Tool. Access to the requested device is then granted for the specified period.

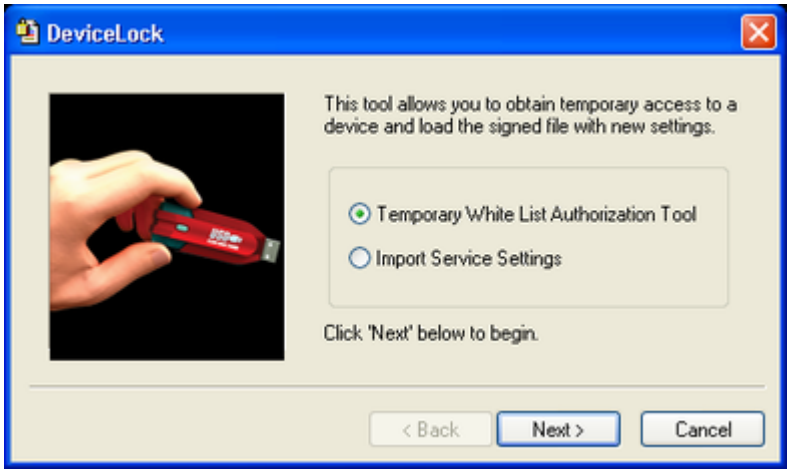
Temporary White List Authorization Tool

The Temporary White List Authorization Tool is a part of the Windows Control Panel applet that users should use to obtain temporary access to devices.

To run the Temporary White List Authorization Tool, the user should run the **DeviceLock** applet from the Control Panel and select the **Temporary White List Authorization Tool** option.

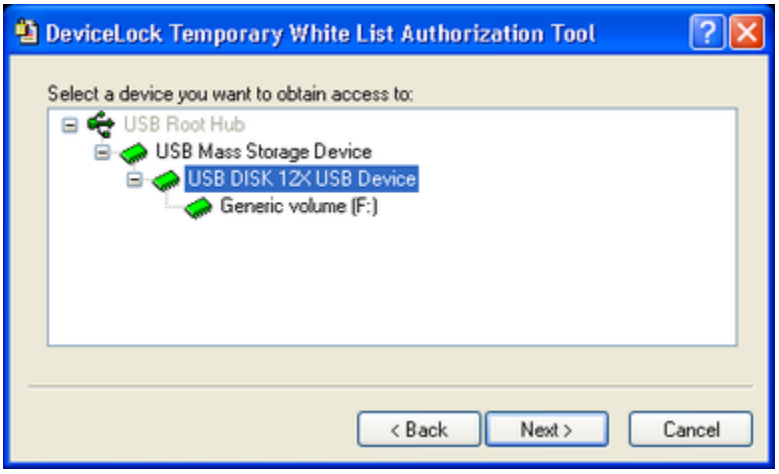


Note: On Windows XP and later, the user must switch the Control Panel to Classic View in order to view all available applets.

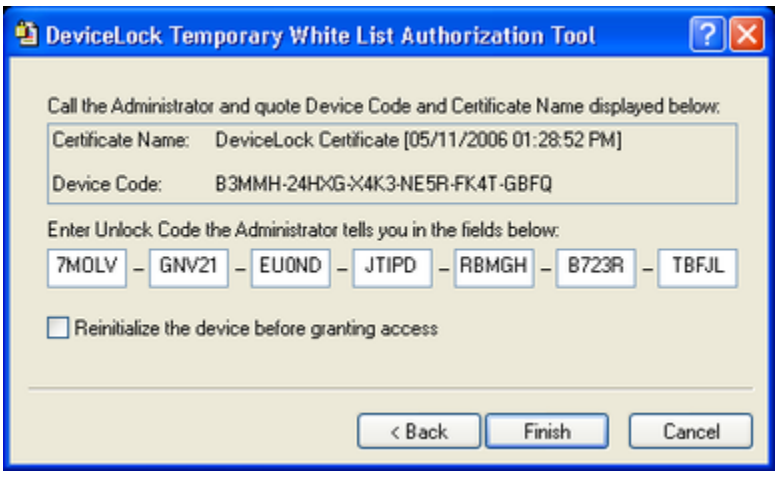

DeviceLock
This tool allows you to obtain temporary access to a device and load the signed file with new settings.
Temporary White List Authorization Tool
Import Service Settings
Click 'Next' below to begin.
< Back
Next >
Cancel

There are five simple steps for the user to request and obtain temporary access to a device:

1. Plug the needed device into the USB port.
2. Select the device from the list of all available USB devices.


DeviceLock Temporary White List Authorization Tool
Select a device you want to obtain access to:
USB Root Hub
USB Mass Storage Device
USB DISK 1.2 USB Device
Generic volume (F:)
< Back
Next >
Cancel

3. Contact an Administrator and tell him/her the name of the certificate and the **Device Code**. Please note that the **Device Code** is only valid within 24 hours of the time it was generated by the applet.


DeviceLock Temporary White List Authorization Tool
Call the Administrator and quote Device Code and Certificate Name displayed below:
Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]
Device Code: B3MMH-24HXG-X4K3-NE5R-FK4T-GBFQ
Enter Unlock Code the Administrator tells you in the fields below:
7MOLV - GNV21 - EU0ND - JTIPD - RBMGH - B723R - TBFJL
Reinitialize the device before granting access
< Back
Finish
Cancel

4. Enter an **Unlock Code** received from the Administrator.

   If it is necessary to force the requested device to reinitialize (replug) before allowing access to it, select the **Reinitialize device before granting access** check box.

   Some USB devices (like the mouse) will not work without being reinitialized, so it is recommended to keep this check box selected for non-storage devices.

   It is recommended to keep the **Reinitialize device before granting access** check box unselected for storage devices (such as flash drives, Optical Drives, external hard drives and so on).

   Some USB devices cannot be reinitialized from DeviceLock Service. It means that their drivers do not support the software replug. If such a device was white listed but does not work, the user should remove it from the port and then insert it back manually to restart the device's driver.

5. Press the **Finish** button.

   *If the **Unlock Code** is valid, then access to the device will be provided in several seconds.*

All successful attempts to add devices to a Temporary White List are logged, if logging of changes is enabled in Service Options.

Appendix

Permissions and Audit Examples for Devices

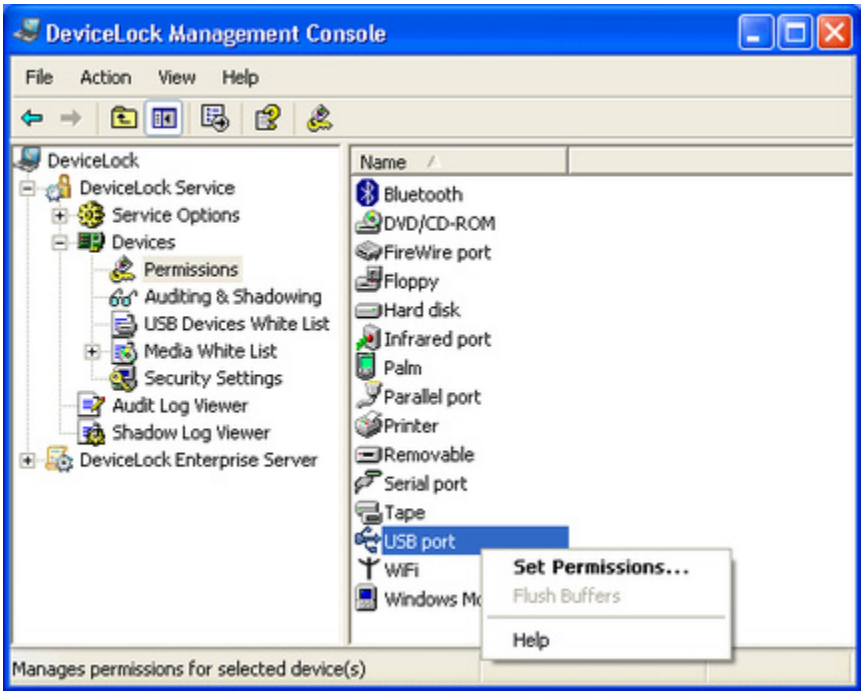
Using the following examples you can better understand how to properly define permissions, audit and shadowing rules in DeviceLock.

All examples assume that you are using DeviceLock Management Console (the MMC snap-in) and it is already connected to the computer where DeviceLock Service is running. For more information on how to use DeviceLock Management Console, see "DeviceLock Management Console."

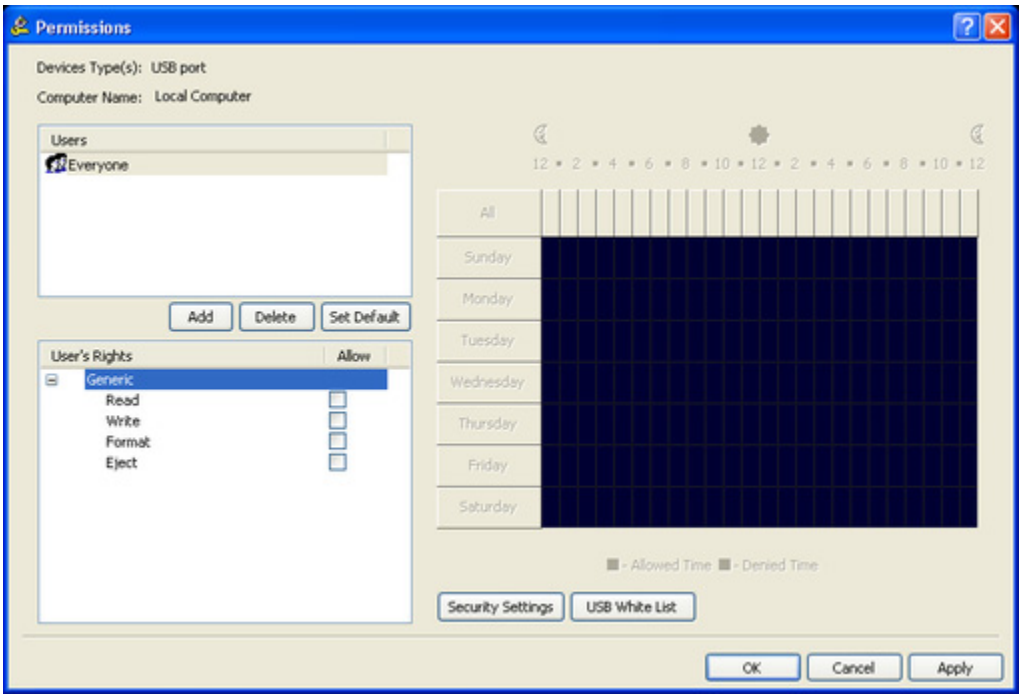
Permissions Examples

For all users all USB devices are denied except the mouse and keyboard:

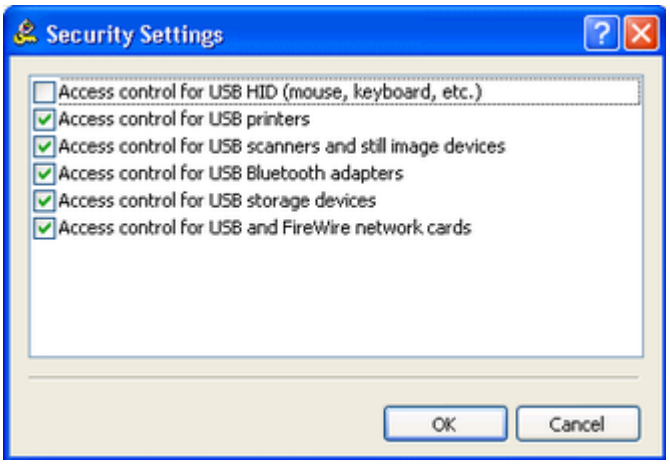
1. Select the **USB port** record from the list of device types under **Permissions**, and then select **Set Permissions** from the context menu available by a right mouse click.



2. Click the **Add** button in the **Permissions** dialog box, add the **Everyone** user (type the name or browse for all available names and select the needed one), click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and disable all rights in the **User's Rights** list.



3. Click the **Security Settings** button in the **Permissions** dialog box, and then clear the **Access control for USB HID (mouse, keyboard, etc.)** check box.

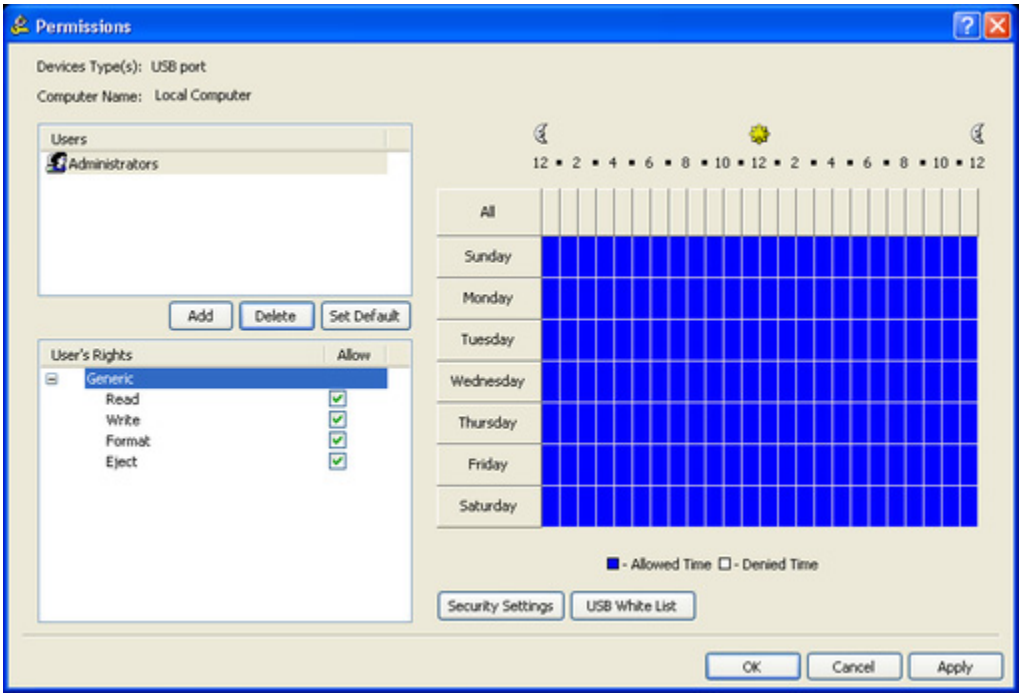

Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

4. Click **OK** to close the **Security Settings** dialog box, click **OK** to apply changes and close the **Permissions** dialog box, and then click **Yes** to confirm that you really want to deny all users access to the USB port.

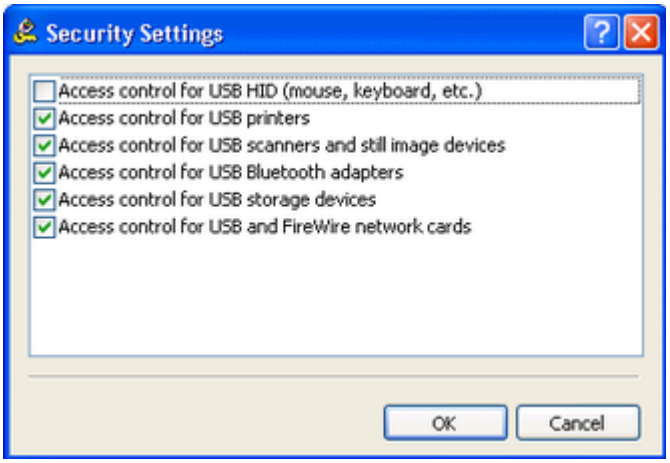
For all users all USB devices are denied except the mouse and keyboard but members of the Administrators group can use all USB devices:

1. Select the **USB port** record from the list of device types under **Permissions**, and then select **Set Permissions** from the context menu available by a right mouse click.

2. Click the **Add** button in the **Permissions** dialog box, add the **Administrators** group (type the name or browse for all available names and select the needed one), click **OK** to close the **Select Users or Groups** dialog box, select the **Administrators** record and enable all rights in the **User's Rights** list.



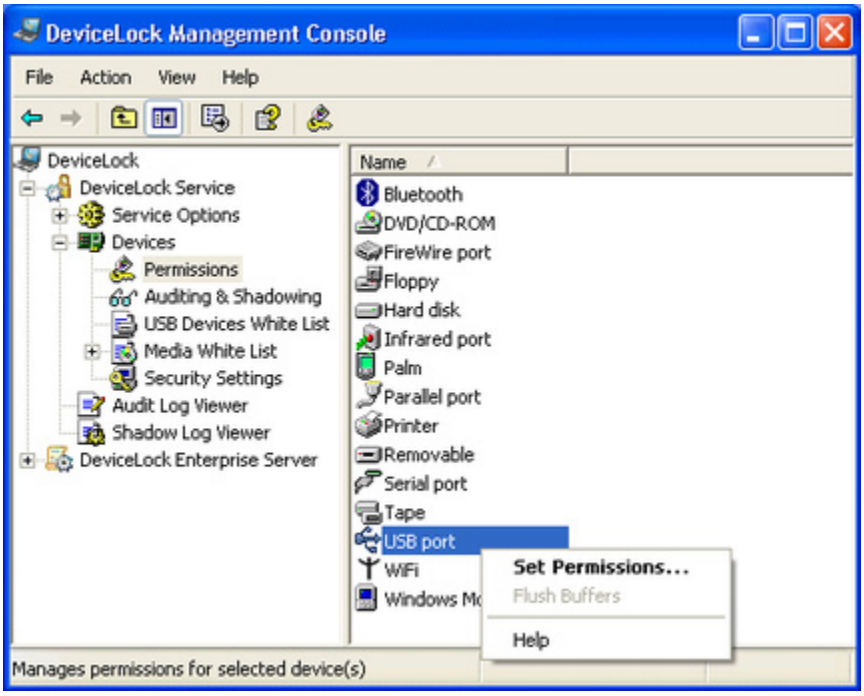
3. Click the **Security Settings** button in the **Permissions** dialog box, and then clear the **Access control for USB HID (mouse, keyboard, etc.)** check box.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

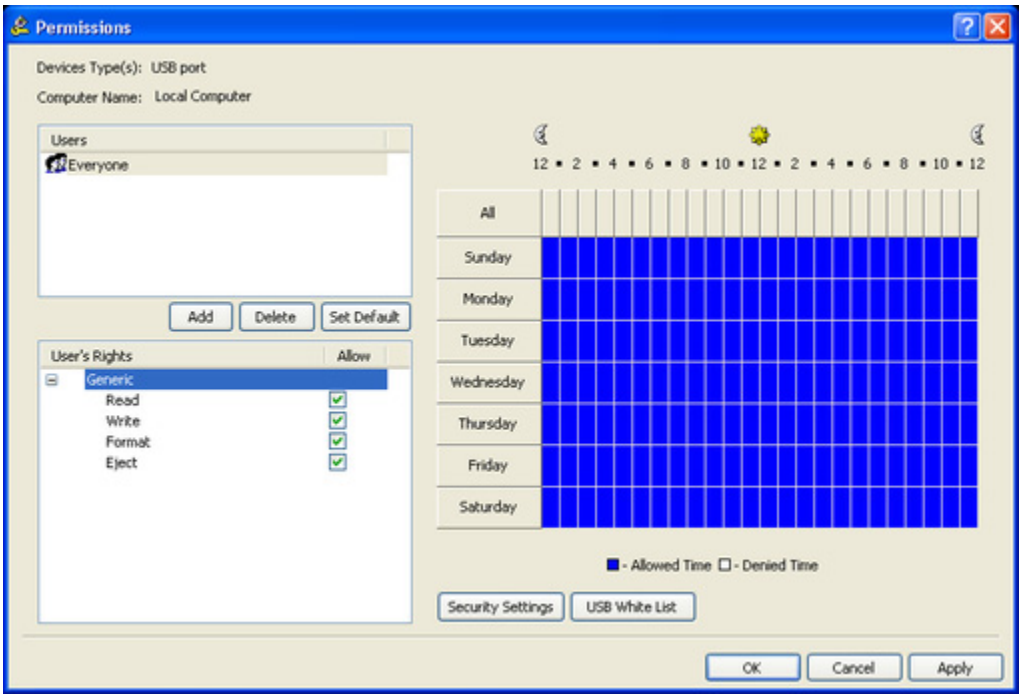
4. Click **OK** to close the **Security Settings** dialog box, and then click **OK** to apply changes and close the **Permissions** dialog box.

For all users all storage devices except fixed hard drives are denied but all non-storage USB devices are allowed:

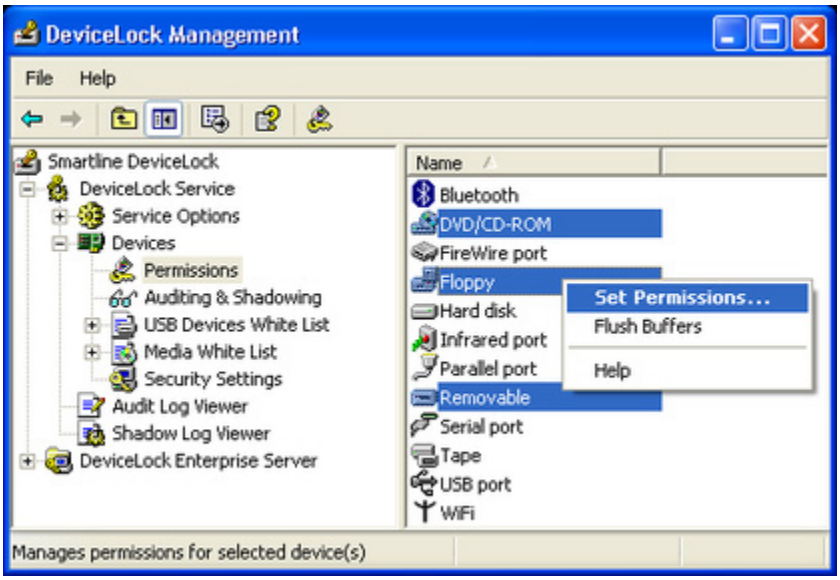
1. Select the **USB port** record from the list of device types under **Permissions**, and then select **Set Permissions** from the context menu available by a right mouse click.



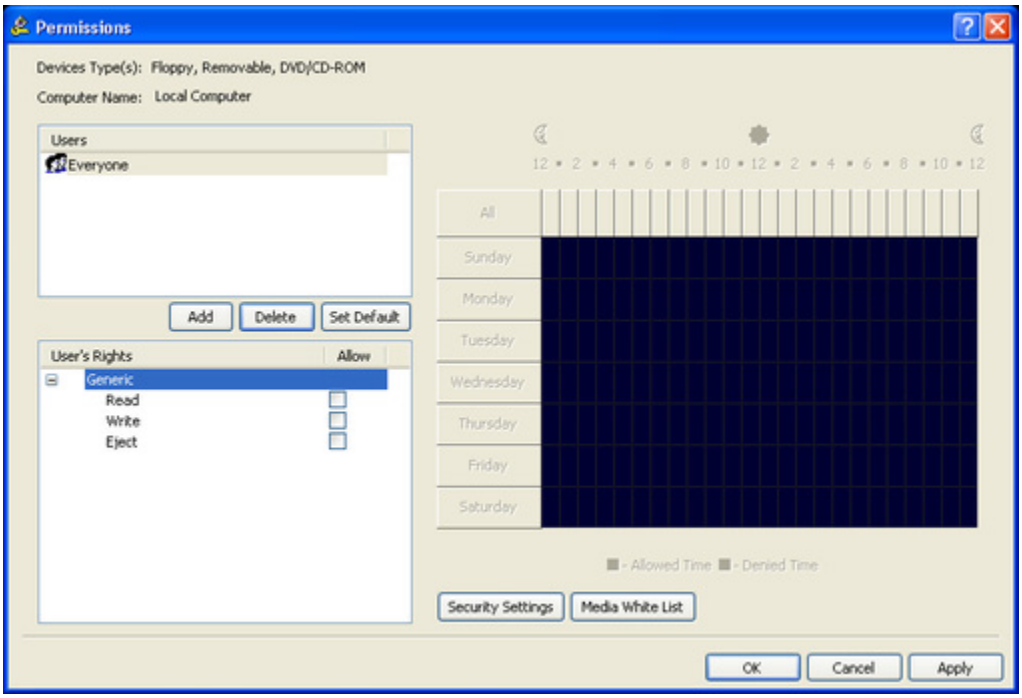
2. Click the **Add** button in the **Permissions** dialog box, add the **Everyone** user (type the name or browse for all available names and select the needed one), click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and enable all rights in the **User's Rights** list.



3. Click **OK** to apply changes and close the **Permissions** dialog box.
4. Select **Optical Drive**, **Floppy** and **Removable** records from the list of device types under **Permissions**, and then select **Set Permissions** from the context menu available by a right mouse click.



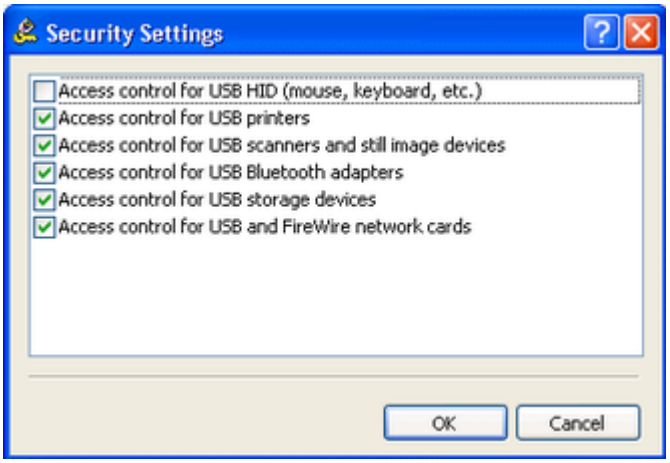
5. Click the **Add** button in the **Permissions** dialog box, add the **Everyone** user (type the name or browse for all available names and select the needed one), click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and disable all rights in the **User's Rights** list.



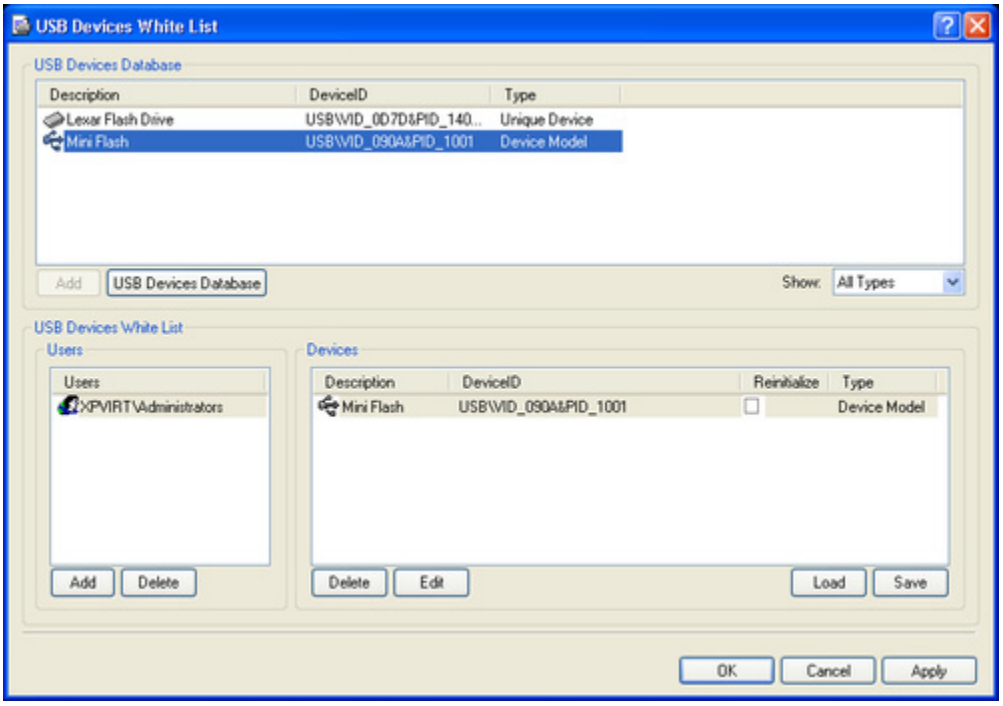
6. Click **OK** to apply changes and close the **Permissions** dialog box, and then click **Yes** to confirm that you really want to deny access to these devices for all users.

For all users all USB devices are denied except the mouse and keyboard but members of the Administrators group can use an authorized model of USB storage devices:

1. Select the **USB port** record from the list of device types under **Permissions**, and then select **Set Permissions** from the context menu available by a right mouse click.
2. Click the **Add** button in the **Permissions** dialog box and add the **Everyone** user (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and disable all rights in the **User's Rights** list.
3. Click the **Security Settings** button in the **Permissions** dialog box, and then clear the **Access control for USB HID (mouse, keyboard, etc.)** check box.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

4. Click **OK** to close the **Security Settings** dialog box, and then click the **USB White List** button in the **Permissions** dialog box.
5. Click the **Add** button below the **Users** list, add the **Administrators** group (type the name or browse for all available names and select the needed one), click **OK** to close the **Select Users or Groups** dialog box, and then select the **Administrators** record.
6. Select the device model's record in the **USB Devices Database** list, and then click the **Add** button below this list.

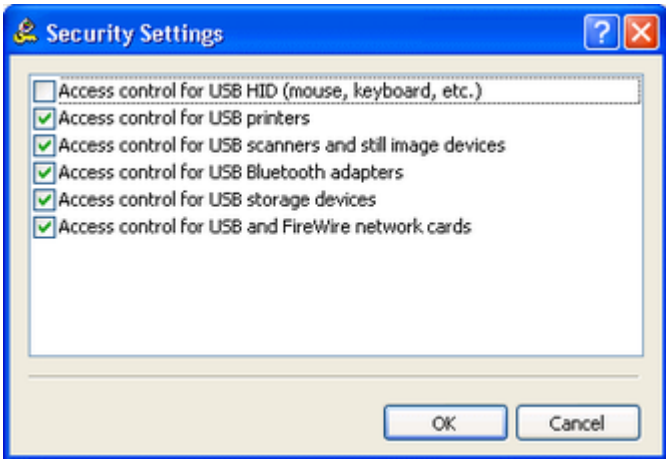


If you do not have devices in the **USB Devices Database** list, click the **USB Devices Database** button below this list, and then add devices as described in the "USB Devices Database" section of this manual. When you finished adding devices to the database, click **OK** to save this database and close the **USB Devices Database** dialog box.

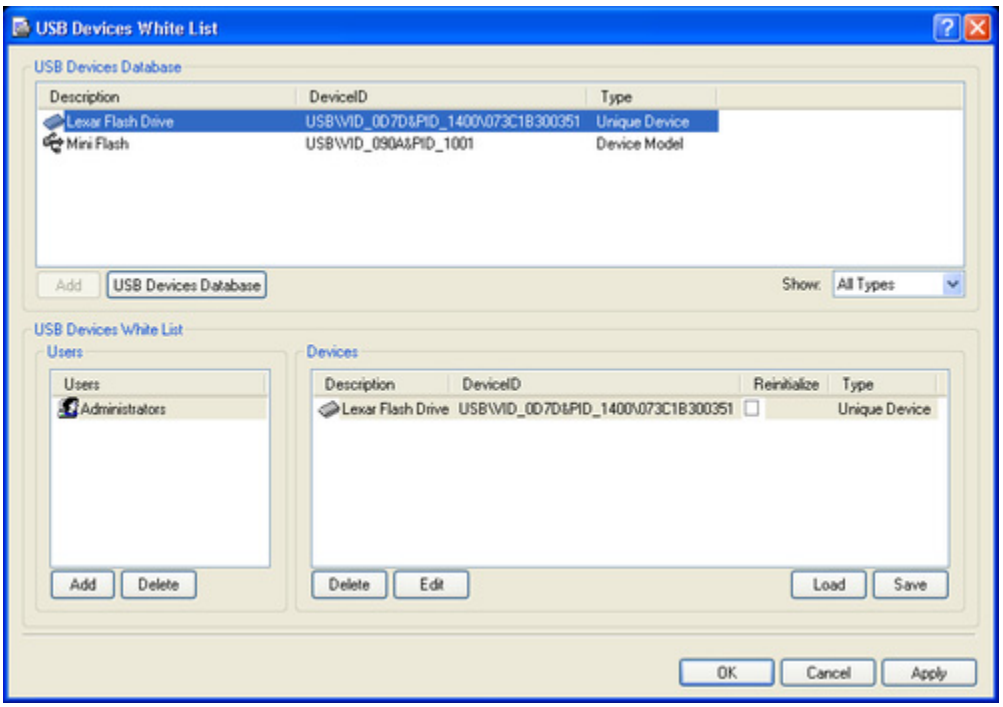
7. Click **OK** to apply the white list settings and close the **USB Devices White List** dialog box, click **OK** to apply changes and close the **Permissions** dialog box, and then click **Yes** to confirm that you really want to deny all users access to the USB port.

For all users all USB devices are denied except the mouse and keyboard but members of the Administrators group can use an authorized unique USB storage device:

1. Select the **USB port** record from the list of device types under **Permissions**, and then select **Set Permissions** from the context menu available by a right mouse click.
2. Click the **Add** button in the **Permissions** dialog box and add the **Everyone** user (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and disable all rights in the **User's Rights** list.
3. Click the **Security Settings** button in the **Permissions** dialog box, and then clear the **Access control for USB HID (mouse, keyboard, etc.)** check box.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

4. Click **OK** to close the **Security Settings** dialog box, and then click the **USB White List** button in the **Permissions** dialog box.
5. Click the **Add** button below the **Users** list and add the **Administrators** group (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, and then select the **Administrators** record.
6. Select the unique device's record in the **USB Devices Database** list, and then click the **Add** button below this list.

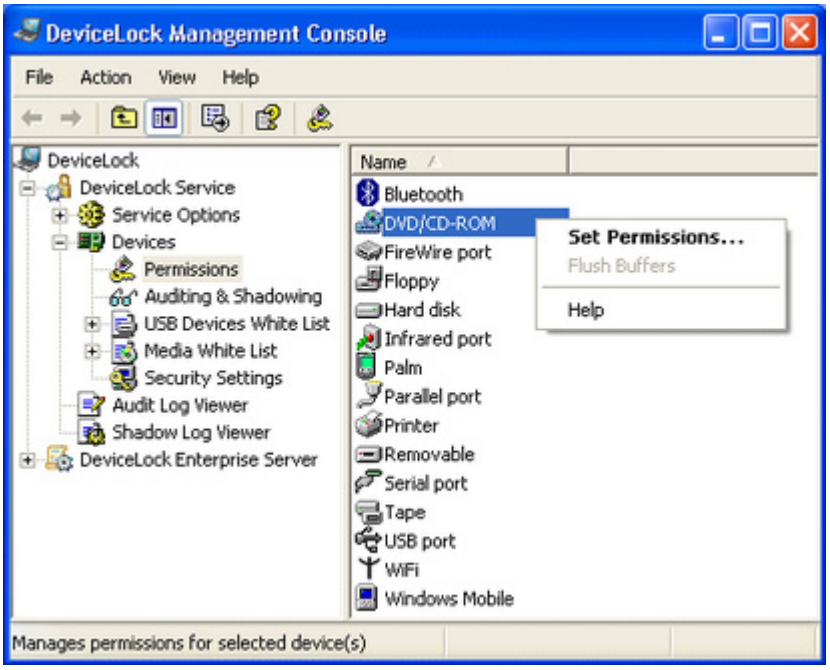


If you do not have devices in the **USB Devices Database** list, click the **USB Devices Database** button below this list, and then add devices as described in the "USB Devices Database" section of this manual. When you finish adding devices to the database, click **OK** to save this database and close the **USB Devices Database** dialog box.

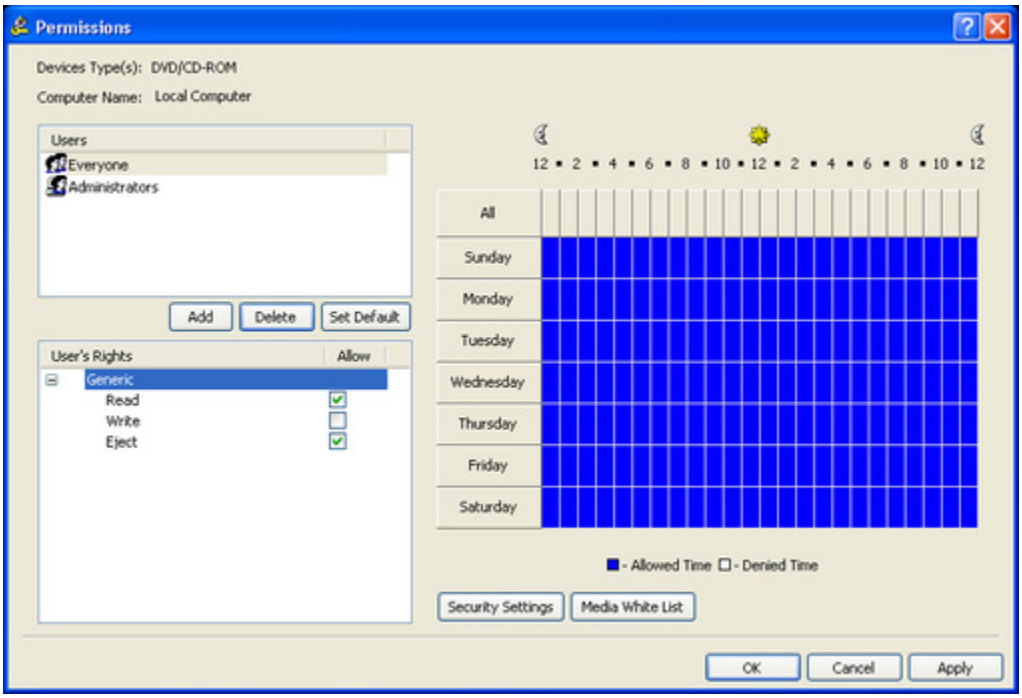
7. Click **OK** to apply the white list settings and close the **USB Devices White List** dialog box, click **OK** to apply changes and close the **Permissions** dialog box, and then click **Yes** to confirm that you really want to deny all users access to the USB port.

For all users all CD/DVD/BD drives are set to the read-only mode but members of the Administrators group can burn (write) CD/DVD/BD disks:

1. Select the **Optical Drive** record from the list of device types under **Permissions**, and then select **Set Permissions** from the context menu available by a right mouse click.



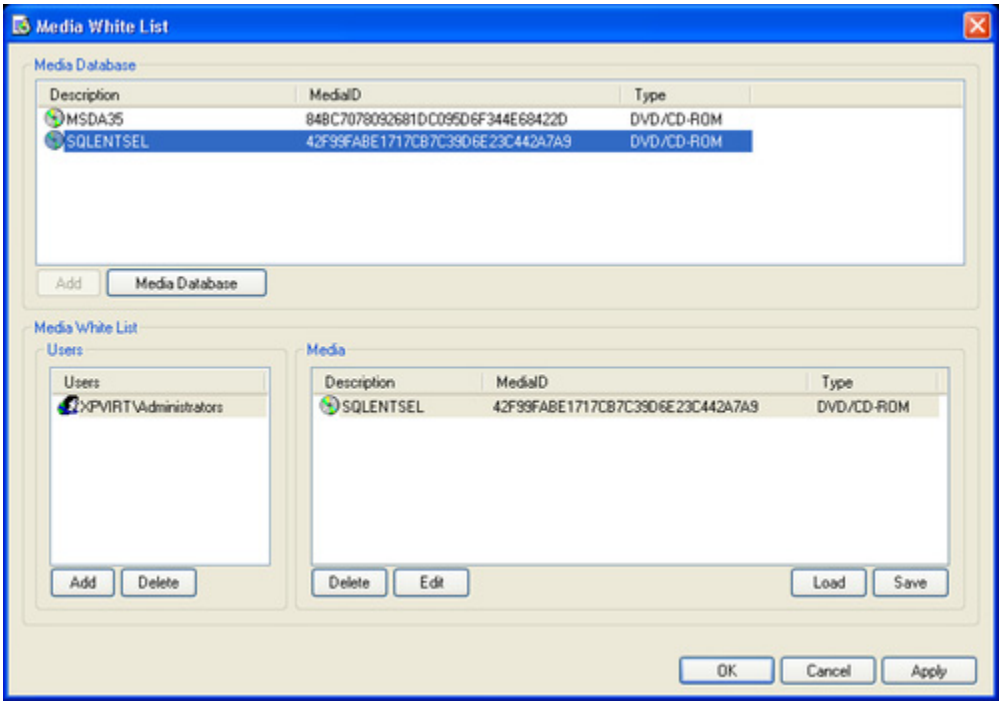
2. Click the **Add** button in the **Permissions** dialog box and add the **Administrators** group (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Administrators** record and enable all rights in the **User's Rights** list.
3. Click the **Add** button in the **Permissions** dialog box and add the **Everyone** user (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box. Select the **Everyone** record and disable the **Write** right in the **User's Rights** list.



4. Click **OK** to apply changes and close the **Permissions** dialog box.

For all users all CD/DVD/BD drives are denied but members of the Administrators group can read a certain disk:

1. Select the **Optical Drive** record from the list of device types under **Permissions**, and then select **Set Permissions** from the context menu available by a right mouse click.
2. Click the **Add** button in the **Permissions** dialog box and add the **Everyone** user (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and disable all rights in the **User's Rights** list.
3. Click the **Media White List** button in the **Permissions** dialog box.



4. Click the **Add** button below the **Users** list and add the **Administrators** group (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, and then select the **Administrators** record.
5. Select the media's record in the **Media Database** list, and then click the **Add** button below this list.

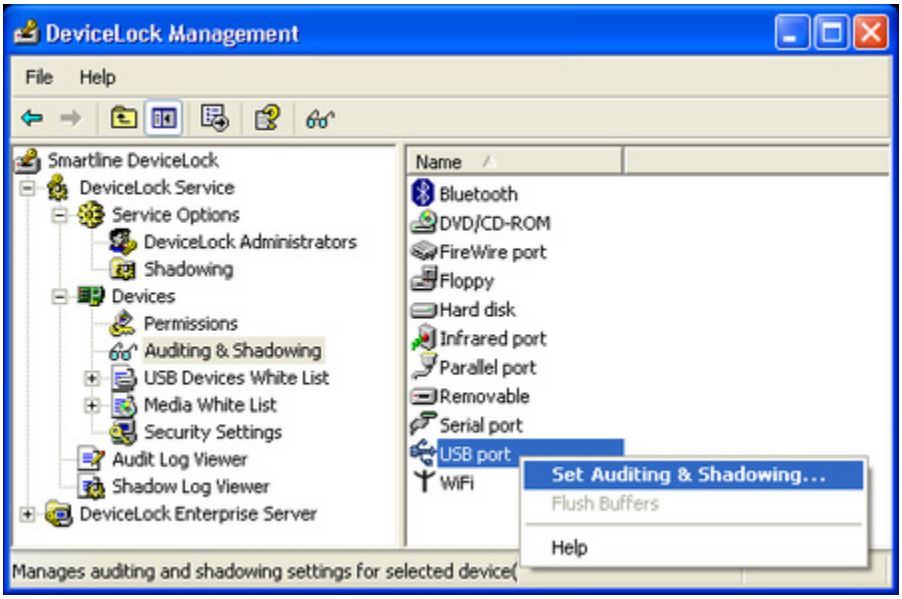
   If you do not have records in the **Media Database** list, click the **Media Database** button below this list, and then authorize a media as described in the "Media Database" section of this manual. When you finish authorizing a media, click **OK** to save the database and close the **Media Database** dialog box.

6. Click **OK** to apply the white list settings and close the **Media White List** dialog box. Click **OK** to apply changes and close the **Permissions** dialog box. Then click **Yes** to confirm that you really want to deny access to CD/DVD/BD drives for all users.

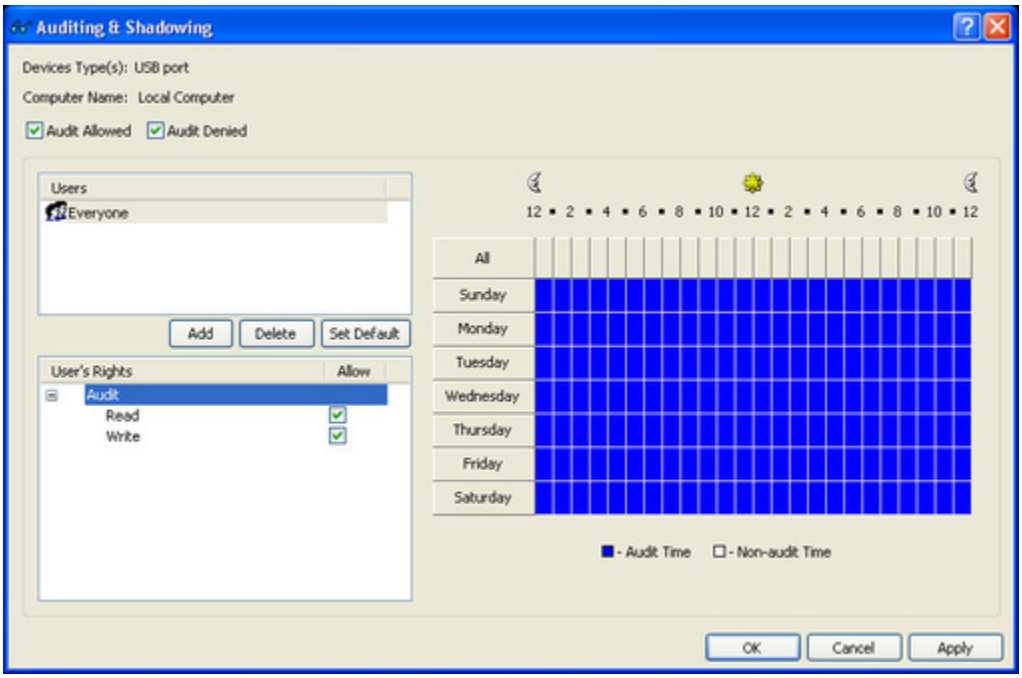
Audit & Shadowing Rules Examples

Log insert, remove and access actions for USB devices for all users:

1. Select the **USB port** record from the list of device types under **Auditing, Shadowing & Alerts**, and then select **Set Auditing, Shadowing & Alerts** from the context menu available by a right mouse click.



2. Click the **Add** button in the **Audit** dialog box and add the **Everyone** user (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and enable **Read** and **Write** audit rights in the **User's Rights** list.

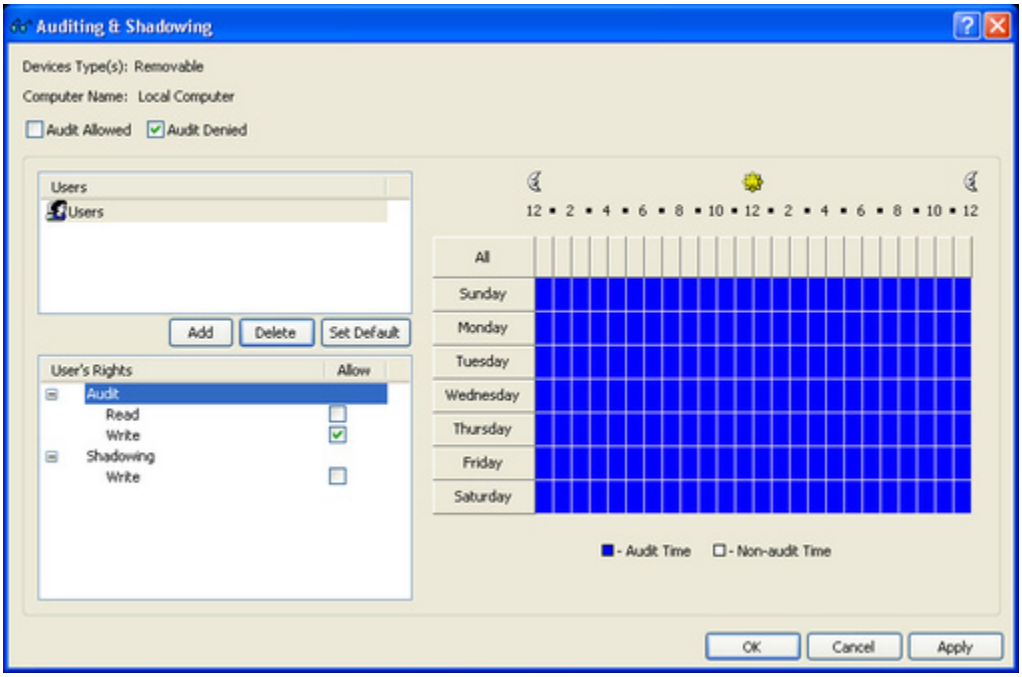


3. Select the **Audit Allowed** and **Audit Denied** check box at the top of the **Audit** dialog box, and then click **OK** to apply changes and close the **Auditing, Shadowing & Alerts** dialog box.

Log only files and folders names related to denied write actions for removable storage devices for members of the Users group:

1. Select the **Removable** record from the list of device types under **Auditing, Shadowing & Alerts**, and then select **Set Auditing, Shadowing & Alerts** from the context menu available by a right mouse click.

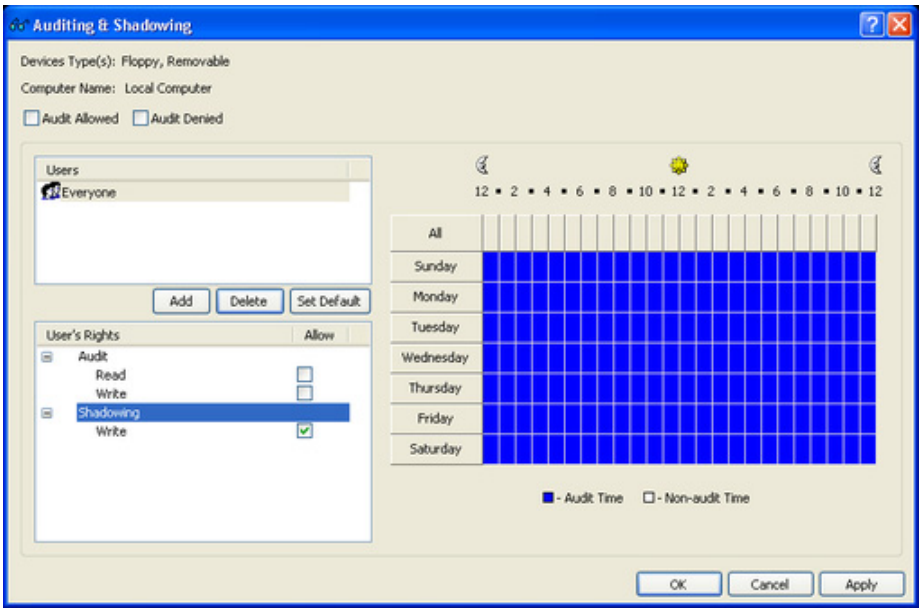
2. Click the **Add** button in the **Audit** dialog box and add the **Users** group (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Users** record and enable only the **Write** audit right in the **User's Rights** list.



3. Select only the **Audit Denied** check box at the top of the **Audit** dialog, and then click **OK** to apply changes and close the **Auditing, Shadowing & Alerts** dialog box.
4. Enable the **Audit folder operations** parameter under **Auditing & Shadowing** in **Service Options**.

Shadow all data writing to removable storage devices and floppies for all users:

1. Select **Floppy** and **Removable** records from the list of device types under **Auditing, Shadowing & Alerts**, and then select **Set Auditing, Shadowing & Alerts** from the context menu available by a right mouse click.
2. Click the **Add** button in the **Audit** dialog box and add the **Everyone** user. Click **OK** to close the **Select Users or Groups** dialog box and select the **Everyone** record. Disable all audit rights and enable only the **Write** shadowing right in the **User's Rights** list.



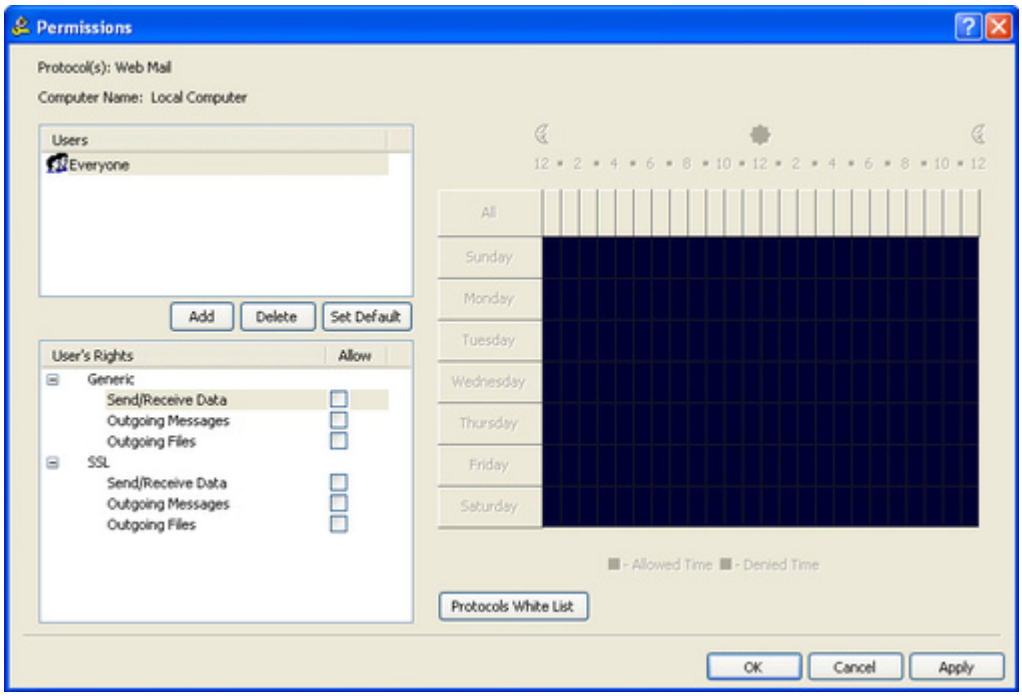
3. Click **OK** to apply changes and close the **Auditing, Shadowing & Alerts** dialog box.

Permissions Examples for Protocols

For all users all Webmail services are denied, but members of the Administrators group can access Gmail:

1. In the console tree, expand **DeviceLock Service**, and then expand **Protocols.**
2. Under **Protocols**, select **Permissions**.
3. In the details pane, right-click **Web Mail**, and then click **Set Permissions**.
4. In the **Permissions** dialog box, do the following:
   a) Under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Everyone**, and then click **OK**.
   b) Under **Users**, select **Everyone**.

c) Under **User's Rights**, select **Deny** for all rights.

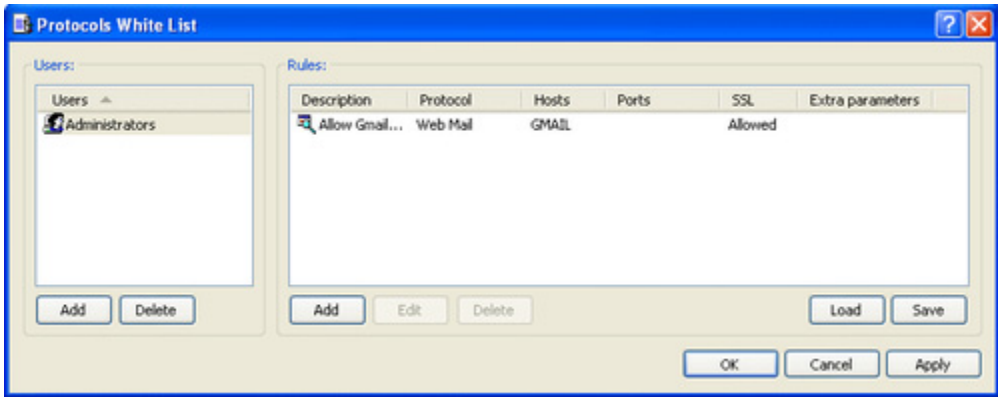


d) Click **Protocols White List**.

5. In the **Protocols White List** dialog box, do the following:

a) Under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Administrators**, and then click **OK**.

b) Under **Users**, select **Administrators**, and then, under **Rules**, click **Add**. In the **Add Rule** dialog box, in the **Description** box, specify the rule name. Next, under **Web Mail services**, select the **Gmail** check box, and then click **OK.**

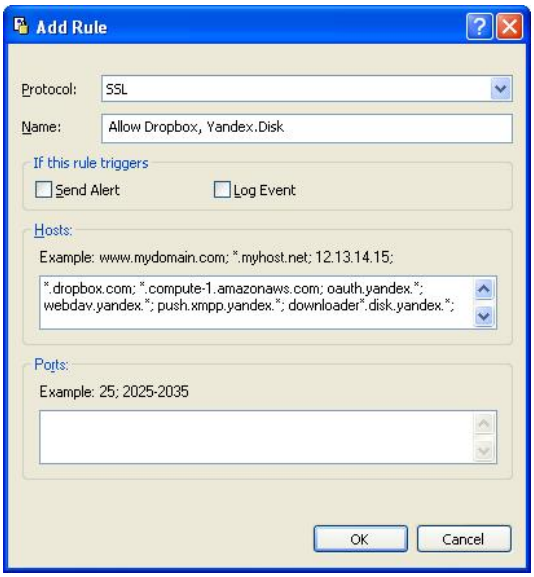


c) Click **OK** or **Apply** to apply the white list settings and close the **Protocols White List** dialog box.

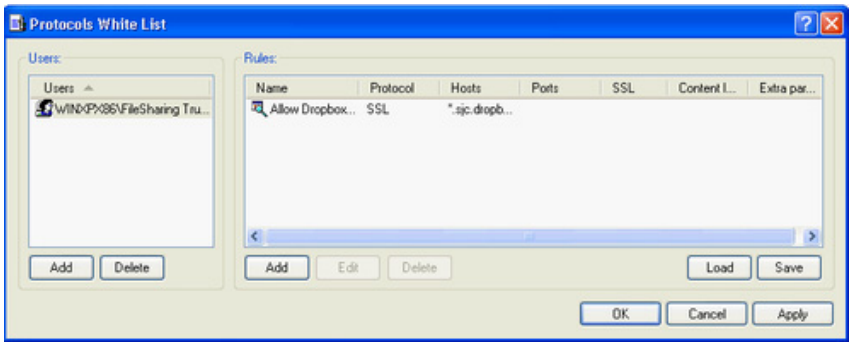
6. In the **Permissions** dialog box, click **OK** or **Apply**.

Members of the FileSharing Trusted Users group are allowed to use Windows-based applications for Dropbox and Yandex.Disk regardless of the permissions set for File Sharing:

1. In the console tree, expand **DeviceLock Service**, and then expand **Protocols**.
2. Under **Protocols**, right-click **White List**, and then click **Manage**.
3. In the **Protocols White List** dialog box, do the following:
   a) Under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **FileSharing Trusted Users**, and then click **OK**.
   b) Under **Users**, select **FileSharing Trusted Users**, and then, under **Rules**, click **Add**.
4. In the **Add Rule** dialog box, do the following:
   a) In the **Protocol:** list, click **SSL**.
   b) In the **Name** box, specify the rule name.
   c) In the **Hosts:** box, type the following DNS names of the Dropbox and Yandex.Disk servers separated by a comma or semicolon:
   Dropbox: ***.dropbox.com** and ***.compute-1.amazonaws.com**
   YandexDisk: **oauth.yandex.***; **webdav.yandex.***; **push.xmpp.yandex.***; **downloader*.disk.yandex.***; **uploader*.disk.yandex.*, *.storage.yandex.***



   d) Click **OK**.



5. Click **OK** or **Apply** to apply the white list settings and close the **Protocols White List** dialog box.

Notes: Access control, auditing, shadowing and content inspection will be disabled for all data transfers.

Content-Aware Rules Examples

All users are denied the right to copy to devices (Floppy, Removable) and transmit over the network (over HTTP, FTP, SMTP, Web Mail) the following types of content: files containing more than 1 credit card number, password-protected documents and archives, files containing more than 1 Social Security number, and images containing a large amount of text.

1. In the console tree, expand **DeviceLock Service**, expand **Devices**, right-click **Content-Aware Rules**, and then click **Manage**.
2. In the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Document Properties**.
3. In the **Add Document Properties Group** dialog box, do the following:
   a) In the **Name** box, specify the name of the group, for example, **Password-protected documents and archives**.
   b) Select the **Password protected** check box.
   c) Click **OK**.

   The new content group you created is added to the existing list of content groups under Content Database in the Content-Aware Rules for Devices dialog box. This group will be used to control access to password-protected documents and archives.
4. In the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Document Properties**.
5. In the **Add Document Properties Group** dialog box, do the following:
   a) In the **Name** box, specify the name of the group, for example, **Images contain 70%text**.
   b) Select the **Contains text** check box and specify **70 %**.
   c) Click **OK**.

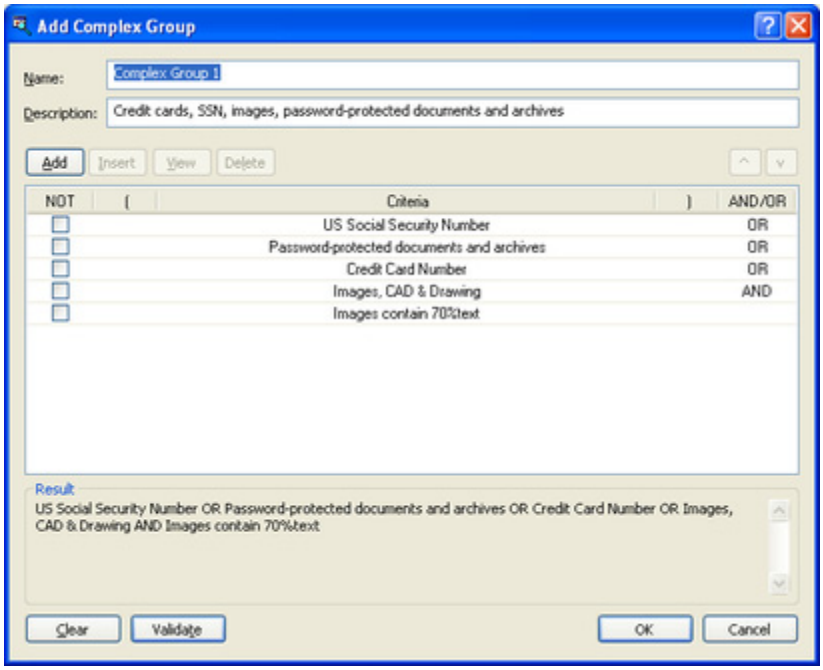
   The new content group you created is added to the existing list of content groups under Content Database in the Content-Aware Rules for Devices dialog box. This group will be used to control access to images containing a large amount of text.
6. In the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Complex**.
7. In the **Add Complex Group** dialog box, do the following:

a) In the **Name** box, specify the name of the group, for example, **Complex Group 1**.

b) Click **Add**. In the **Content Groups** dialog box, select the following groups: **Credit Card Number**, **Images, CAD & Drawing**, **Images contain 70%text**, **Password-protected documents and archives**, and **US Social Security Number**.

You can select these groups simultaneously by holding down the CTRL key while clicking them.

c) Compose the following logical expression: **US Social Security Number OR Password-protected documents and archives OR Credit Card Number OR Images, CAD & Drawing AND Images contain 70%text.**



d) Click **OK**.

The new content group you created is added to the existing list of content groups under Content Database in the Content-Aware Rules for Devices dialog box. This group will be used to control access to files containing more than 1 credit card number, password-protected documents and archives, files containing more than 1 Social Security number, and images containing a large amount of text.

8. In the **Content-Aware Rules for Devices** dialog box, do the following:

   a) Under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Everyone**, and then click **OK**.

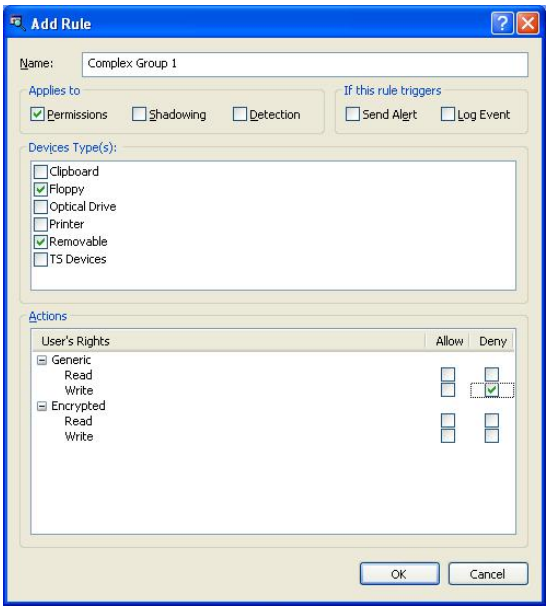
   b) Under **Users**, select **Everyone**. Under **Content Database,** select the **Complex Group 1** content group, and then click **Add**.

9. In the **Add Rule** dialog box, do the following:

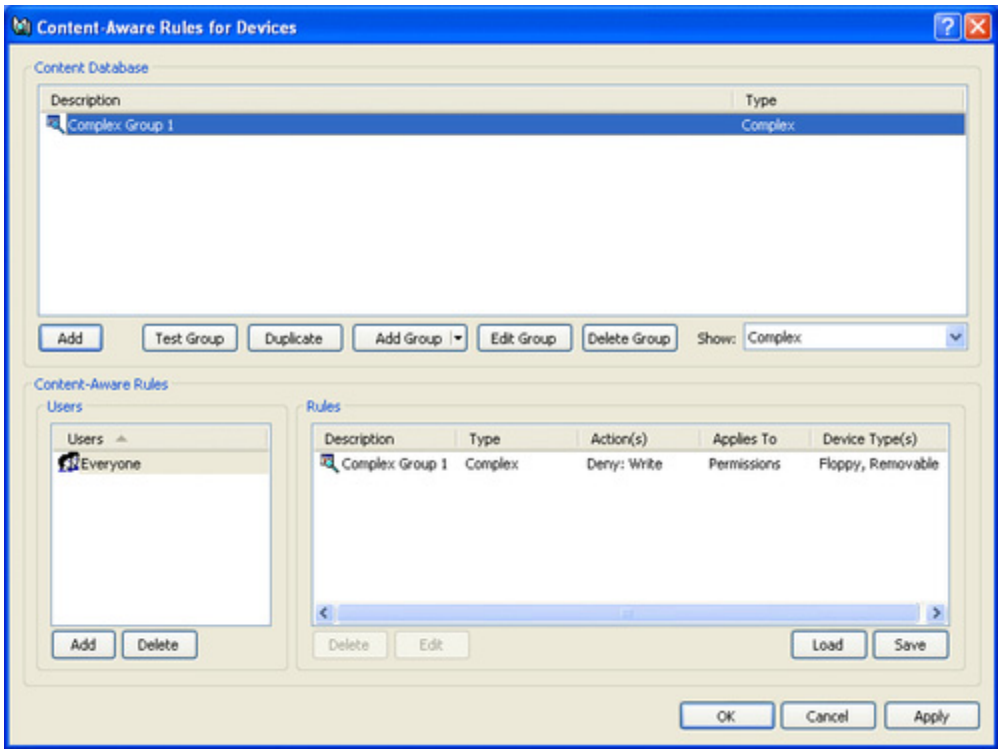
   a) Under **Applies to**, select the **Permissions** check box.

   b) Under **Device Type(s)**, select the **Floppy** and **Removable** check boxes.

   c) Under **Action(s)**, select the **Deny** check box next to **Write**.



d) Click **OK**.



10. In the **Content-Aware Rules for Devices** dialog box, click **OK** or **Apply** to apply the rule.
11. In the console tree, expand **Protocols**, right-click **Content-Aware Rules**, and then click **Manage**.
12. In the **Content-Aware Rules for Protocols** dialog box, do the following:
    a) Under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Everyone**, and then click **OK**.

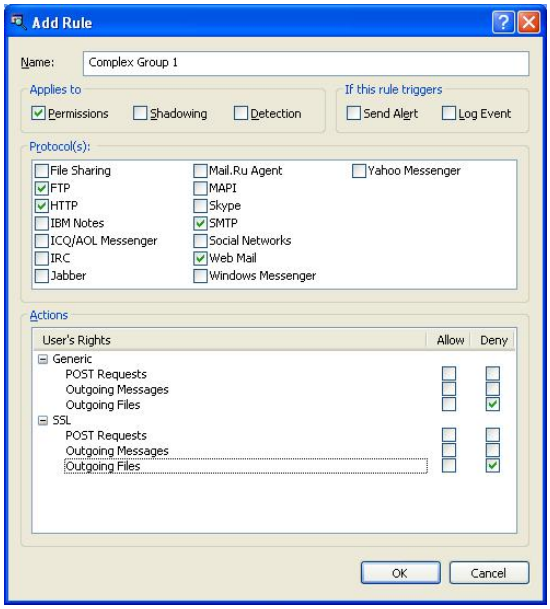
b) Under **Users**, select **Everyone**. Under **Content Database**, select the **Complex Group 1** content group, and then click **Add**.

13. In the **Add Rule** dialog box, do the following:

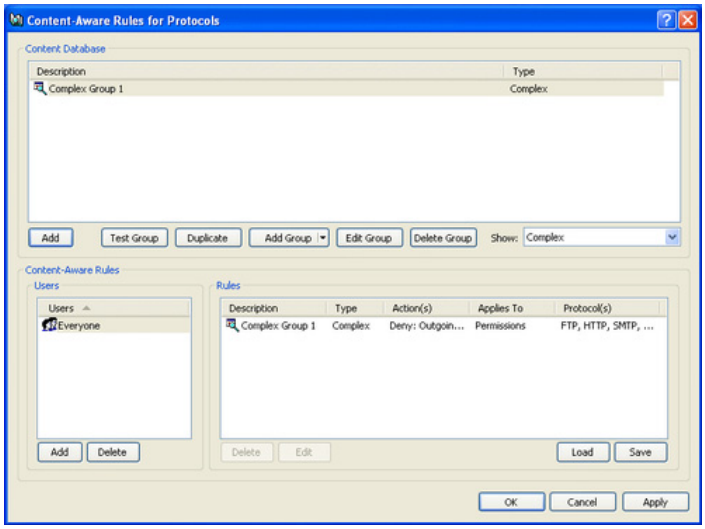
a) Under **Applies to**, select the **Permissions** check box.

b) Under **Protocol(s)**, select the **FTP**, **HTTP**, **SMTP**, and **Web Mail** check boxes.

c) Under **Action(s)**, select the **Deny** check box next to **Generic: Outgoing Files** and **SSL: Outgoing Files.**



d) Click **OK**.



14. In the **Content-Aware Rules for Protocols** dialog box, click **OK** or **Apply** to apply the rule.

Basic IP Firewall Rule Examples

These examples show rules that you can create for the IP Firewall.

The IP firewall is configured to block Remote Desktop connections to the computer where DeviceLock Service is running.

1. In the console tree, expand **DeviceLock Service**, and then expand **Protocols**.
2. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Manage**.
3. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, click **Add**.
4. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **SYSTEM**, and then click **OK**.
5. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select **SYSTEM**.
6. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Add**.
7. In the **Add Rule** dialog box, do the following:
    a) In the **Name** box, specify the name of the firewall rule, for example, **Block RDP**.
    b) Under **Protocol**, select the **TCP** and **UDP** check boxes.
    c) Under **Type**, click **Deny**.
    d) Under **Direction**, select the **Incoming** check box.
    e) In the **Ports** box, type **3389**.
    f) Click **OK**.
8. Click **OK** or **Apply** to apply the firewall rule settings and close the **Basic IP Firewall** dialog box.

The IP firewall is configured to allow incoming Post Office Protocol version 3 (POP3) connections for the specified user, while all other incoming connections to the computer where DeviceLock Service is running are blocked.

1. In the console tree, expand **DeviceLock Service**, and then expand **Protocols**.
2. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Manage**.
3. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, click **Add**.
4. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Everyone**, and then click **OK**.
5. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select **Everyone**.
6. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Add**.
7. In the **Add Rule** dialog box, do the following:
    a) In the **Name** box, specify the name of the firewall rule, for example, **Deny ALL**.
    b) Under **Protocol**, select the **TCP** and **UDP** check boxes.
    c) Under **Type**, click **Deny**.
    d) Under **Direction**, select the **Incoming** check box.

e) In the **Ports** box, type **0-65535**.
f) Click **OK**.

The rule you created is displayed under Rules in the right pane of the Basic IP Firewall dialog box. This rule will be used to block all remote connections to the client computer.

8. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, click **Add**.
9. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user who is allowed to use POP3, and then click **OK**.
10. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user who is allowed to use POP3.
11. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Add**.
12. In the **Add Rule** dialog box, do the following:
    a) In the **Name** box, specify the name of the firewall rule, for example, **Allow POP3 connections**.
    b) Under **Protocol**, select the **TCP** check box.
    c) Under **Type**, click **Allow**.
    d) Under **Direction**, select the **Incoming** check box.
    e) In the **Ports** box, type **110**.
    f) Click **OK**.

    The rule you created is displayed under Rules in the right pane of the Basic IP Firewall dialog box. This rule will be used to unblock port 110 in the firewall to allow incoming POP3 connections for the specified user.
13. Click **OK** or **Apply** to apply the firewall rule settings and close the **Basic IP Firewall** dialog box.

The IP firewall is configured to block all TeamViewer connections to and from the computer where DeviceLock Service is running.

1. In the console tree, expand **DeviceLock Service**, and then expand **Protocols**.
2. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Manage**.
3. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, click **Add**.
4. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Everyone**, and then click **OK**.
5. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select **Everyone**.
6. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Add**.
7. In the **Add Rule** dialog box, do the following:
    a) In the **Name** box, specify the name of the firewall rule, for example, **Deny TeamViewer**.
    b) Under **Protocol**, select the **TCP** check box.
    c) Under **Type**, click **Deny**.
    d) Under **Direction**, select the **Outgoing** check box.

e) In the **Ports** box, type **5938**.
f) Click **OK**.

The rule you created is displayed under Rules in the right pane of the Basic IP Firewall dialog box. This rule will be used to block all TeamViewer connections to its servers.

8. Click **OK** or **Apply** to apply the firewall rule settings and close the **Basic IP Firewall** dialog box.